

"十二五"普通高等教育本科国家级规划教材

普 通 高 等 教 育 精 品 教 材

配套用书



21世纪大学本科计算机专业系列教材

吴 英 编著

计算机网络习题解析与同步练习（第2版）

http://www.tup.com.cn

- 根据教育部"高等学校计算机科学与技术专业规范"组织编写
- 与美国 ACM 和 IEEE CS *Computing Curricula* 最新进展同步
- 国家级精品教材配套用书

清华大学出版社

21世纪大学本科计算机专业系列教材

计算机网络习题解析与同步练习

（第2版）

吴　英　编著

清华大学出版社
北　京

内 容 简 介

本书作为《计算机网络(第4版)》的教学参考书,结合例题解析和同步练习题来复习相关知识点。本书尽可能地考虑选择的同步练习与综合练习题的难度与数量适中,尽量覆盖应知应会的课程内容。通过解析400多道同步练习题和综合练习题,将需要掌握的知识点串联起来。学生结合教学进度,通过同步练习题检查知识掌握的情况,加深对计算机网络知识的理解。根据近年来教学中发现学生在课程考核与研究生入学考试中,对网络综合应用题解决能力较差的现状,第2版重点增加了高层网络综合应用题与习题解析的内容;同时结合计算机网络技术的发展,适度增加了无线局域网Wi-Fi、无线网络与物联网方面的习题。

本书可以作为计算机、软件工程、网络工程、信息安全、物联网工程、传感网技术、通信工程与电子信息等专业教师、学生学习计算机网络课程的参考书,也可作为参加计算机专业硕士研究生全国统考的学生作为复习、考试,以及学生求职应聘准备时的参考书。

图书在版编目(CIP)数据

计算机网络习题解析与同步练习/吴英编著. —2版. —北京:清华大学出版社,2017(2017.12重印)
(21世纪大学本科计算机专业系列教材)
ISBN 978-7-302-46902-5

Ⅰ.①计… Ⅱ.①吴… Ⅲ.①计算机网络－高等学校－习题集 Ⅳ.①TP393-44

中国版本图书馆CIP数据核字(2017)第063953号

责任编辑: 张瑞庆　李　晔
封面设计: 常雪影
责任校对: 李建庄
责任印制: 刘祎淼

出版发行: 清华大学出版社
网　址: http://www.tup.com.cn,http://www.wqbook.com
地　址: 北京清华大学学研大厦A座　**邮　编:** 100084
社 总 机: 010-62770175　**邮　购:** 010-62786544
投稿与读者服务: 010-62776969,c-service@tup.tsinghua.edu.cn
质量反馈: 010-62772015,zhiliang@tup.tsinghua.edu.cn
课件下载: http://www.tup.com.cn,010-62795954
印 装 者: 三河市少明印务有限公司
经　销: 全国新华书店
开　本: 185mm×260mm　**印　张:** 17.25　**字　数:** 415千字
版　次: 2011年6月第1版　2017年6月第2版　**印　次:** 2017年12月第2次印刷
印　数: 1001～2000
定　价: 39.00元

产品编号:069479-01

本书主审：钱德沛

前　言

FOREWORD

随着计算机网络与互联网、移动互联网、物联网技术的发展，计算机网络已经成为计算机与相关专业学生必修的一门基础性的课程，也是全国计算机专业硕士研究生入学统考的课目之一。计算机网络具有交叉学科的性质，对于很多计算机与信息技术专业的学生学习起来是有一定困难的。学习网络课程的困难主要表现在三个方面：一是知识体系庞杂，涉及的面多，很难理出一个头绪；二是网络技术发展、知识更新的速度太快，技术术语很多，非常容易产生混淆；三是对于很多问题，即使课本知识表面上是读懂了，但是遇到问题还是无从下手。作者自己也经过这样一个痛苦的过程，因此对于初学者的困惑也是深有体会的。

作者在与准备参加计算机专业硕士研究生全国统考的同学交流时发现，他们对于统考科目中数据结构、计算机组成原理、操作系统这三门课程都觉得容易复习一些，对于计算机网络课程的复习普遍觉得没把握。作者注意到网络上也有很多这方面的讨论。作者认为产生这个想法是很自然的。因此作者希望《计算机网络习题解析与同步练习(第 2 版)》也可以作为准备参加计算机专业硕士研究生全国统考、求职考试学生的参考资料，也可供信息技术领域的教师、高年级学生、工程技术人员学习和研究网络技术时参考。

为了配合课程教学，帮助读者一步一步地掌握计算机网络知识与技能，作者依据《计算机网络(第 4 版)》的知识体系与教学要求，参考和研究了 Cisco 公司 CCNA/CCNP 培训/考试大纲与试题、计算机专业研究生全国统考大纲与试题、全国计算机等级考试(三级、四级)网络工程师考试大纲与试题，从网上收集了一些计算机、通信与软件产业人员的招聘考题，参考了国内外已经出版的各种习题集。本书写作遵循以下的思路。

1. 结构清晰，覆盖大纲

主教材《计算机网络(第 4 版)》主干部分的特点是突出网络技术中基本知识和技能，同时兼顾无线网络、移动 IP、物联网和新的网络应用技术，本书根据主教材的章节顺序与内容编写同步练习与综合练习，力求做到既能够自成体系，又方便读者对某方面知识的复习与例题的查找。

2. 内容简洁，重点突出

本书不采取通常在每章之前花很大的篇幅去总结和复习知识点的做法，而是按照主教材要求掌握的重点和难点去设计同步练习题。本书尽可能地考虑选择的 400 多道同步练习与 8 个综合练习题，难度与数量适中，尽量覆盖应知应会的课程内容。学生可以根据同步练习题自查知识的掌握情况，不能正确回答的问题可以看同步练习答案与解析。一章结束时，可以通过综合练习题，对一章的内容做一个总结。同步练习题与综合练习题的内容构成了

相对合理的体系。读者在阅读同步练习答案与解析的过程中就可以复习相关章节的主要内容。

同步练习参考了统考试题的命题以及Cisco公司CCNA/CCNP培训/考试大纲与试题、教育部考试中心全国计算机等级考试(三级、四级)网络工程师考试大纲与试题,参考了一些计算机、通信与软件产业人员的招聘考题,参考了国内外已经出版的各种习题集,希望能够通过备考的过程帮助同学掌握知识与技能,提高学生参加研究生考试、通过网络技术认证考试以及就业时的竞争力。书中带*号的习题或例题属于比较难的问题,供基础比较好的读者学习时参考。

3. 适于自学,易读易懂

本书可供教师在教学中参考。任课教师可以根据教学的需要直接使用书中每一章的习题,也可以根据习题与同步练习题改编出新的习题。学生可以在课后通过同步练习题,系统地检查、充实和掌握网络课程的基本知识,为本科网络课程的学习以及准备研究生入学考试、求职考试打下基础。

建议学生根据教学进度,同步选择相应内容的习题,先独立完成,如果有困难再看对应习题的解析;不建议自己没有动手做,就直接看答案。

在完成该书写作之际,作者特别感谢吴功宜教授、徐敬东教授、张建忠教授多年的教诲与帮助,感谢网络实验室张玉老师、许昱玮老师,也要感谢同学们,大家的讨论给了作者很多的灵感、启发与帮助。

由于作者的学识、经验的欠缺,在本书同步练习题的选取与解析等方面,一定会存在很多的不足,诚请老师与同学们指出。

吴　英
wuying@nankai.edu.cn
南开大学
计算机与控制工程学院
计算机与信息安全系
2017年4月

目　录

CONTENTS

第 1 章 计算机网络概论

第一部分 同步练习

1.1 计算机网络的形成与发展

1-1-1 以下关于 ARPANET 网络特征的描述中，错误的是________。

A. ARPANET 的成功运行证明了分组交换理论的正确性

B. ARPANET 为 Internet 的形成奠定了基础

C. Web 应用促进了 ARPANET 的发展

D. ARPANET 采用的是 TCP/IP 协议标准

1-1-2 以下关于计算机网络与 Internet 特征的描述中，错误的是________。

A. 数据通信技术为计算机网络的形成奠定技术基础

B. 分组交换概念奠定计算机网络的理论基础

C. OSI 参考模型成为 Internet 核心协议

D. Web 应用对 Internet 的发展起到了重要的推动作用

1-1-3 以下关于移动互联网特点的描述中，错误的是________。

A. 移动 IP 与无线通信技术的研究为移动互联网发展奠定了坚实基础

B. 移动通信网与互联网业务的融合为移动互联网开辟了广阔的发展空间

C. 智能手机、可穿戴计算等智能终端设备的应用促进了移动互联网应用的快速发展

D. 无线自组网与无线传感器网络成为移动互联网应用的基本模式

1-1-4 以下关于物联网特点的描述中，错误的是________。

A. 现实物理世界与网络虚拟世界融合的需求促进了物联网概念的形成与研究的发展

B. 感知、智能与网络技术的融合为物联网的发展奠定了技术基础

C. 物联网智能终端设备基本上都是在智能手机基础上开发出来的

D. 物联网为计算机网络技术研究提供了更大发展空间

1-1-5 以下关于计算机网络发展趋势的描述中，错误的是________。

A. 计算机网络正在沿着“互联网—移动互联网—物联网”的轨迹发展

B. 移动互联网的作用是扩大了信息共享的深度与灵活性
C. 物联网扩大了人类对现实社会感知与智能处理能力
D. 遵循“三网融合”的模式推动着社会发展

1.2 计算机网络技术发展的三条主线

1-2-1 以下关于 ARPANET—TCP/IP—Internet 发展过程的描述中,错误的是________。
A. ARPANET 的研究奠定了 Internet 发展的基础,而二者共同的发展基础是 IEEE 802 协议体系
B. 广域网、城域网与局域网技术的成熟加速了 Internet 的发展进程
C. 计算机网络、电信网络与有线电视网络从结构、技术到服务呈现出三网融合的趋势
D. P2P 模式进一步扩大了网络资源共享范围和深度

1-2-2 以下关于“从无线分组网到无线自组网、无线传感器网络”发展过程的描述中,错误的是________。
A. 无线网络分为需要基站的基于基础设施与不需要基站的无基础设施的两类
B. 802.11 既可以需要基础设施也可以不需要基站(无基础设施)
C. 802.16 无线城域网属于不需要基础设施的无线网络
D. 无线传感器网将无线自组网与传感器技术结合起来

1-2-3 以下关于网络安全技术特点的描述中,错误的是________。
A. “网络空间”是一个国家的第五个疆域
B. 网络攻击已经逐步发展到有组织的经济犯罪
C. TCP/IP 协议对预防网络攻击有保护作用
D. 网络安全性取决于链条中最薄弱的环节

1-2-4 网络安全是一个系统的社会工程,它不涉及________。
A. 技术　　B. 资源　　C. 法律　　D. 道德

1.3 计算机网络定义与分类

1-3-1 以下关于计算机网络定义的描述中,错误的是________。
A. 以能够相互共享资源的方式互联起来的自治计算机系统的集合
B. 网络共享的资源主要指计算机的 CPU、内存与操作系统
C. 互联的计算机既可以联网工作,也可以脱网单机工作
D. 联网计算机之间的通信必须遵循共同的网络协议

1-3-2 以下关于按传输技术对网络进行分类的描述中,错误的是________。
A. 通信信道的类型有两类:广播通信信道与点对点通信信道
B. 网络也可以分为广播式网络与点对点式网络
C. 广播式网络中所有联网计算机都共享一个公共的通信信道
D. 点对点式网络必须采用存储转发与介质访问控制机制

1-3-3 以下术语的解析中,错误的是________。
A. internet 指的是将多个计算机网络互联成大型网络系统的技术

B. Internet 是 internet 中的一种网络

C. internet 也是 Internet 中的一种网络

D. Intranet 不连接或不直接连接到 Internet

1-3-4 以下不属于按覆盖范围分类的计算机网络类型的是________。

A. 广域网　　B. 城域网　　C. 局域网　　D. 接入网

1-3-5 以下关于广域网 WAN 特点的描述中，错误的是________。

A. 在 Internet 中广域网要实现广域网与广域网、广域网与城域网的互联

B. 广域网与广域网的互联构成了 Internet 的核心主干网

C. 广域网技术研究的重点要放在接入技术上

D. 广域网是一种公共数据网络

1-3-6 以下关于宽带城域网 MAN 特点的描述中，错误的是________。

A. 电信、有线电视与计算机网络在电话业务上的融合成为宽带城域网的核心业务

B. 宽带城域网的网络平台是由核心交换层、汇聚层与接入层组成的

C. 城域网通过城市宽带出口接入国家主干网

D. 完善的光纤传输网是宽带城域网的基础

1-3-7 以下关于局域网 LAN 特点的描述中，错误的是________。

A. 局域网适用于机关、校园、工厂等有限范围内的计算机联网

B. 局域网还可以用于构建存储区域网络、云计算服务器集群的后端网络

C. 局域网能够提供高达 10Gbps 的数据传输速率

D. 最流行的局域网是 Ethernet 与 Wi-Fi

1-3-8 以下关于无线个人区域网 WPAN 特点的描述中，错误的是________。

A. 个人区域网(PAN)主要是用无线通信技术实现联网设备之间的通信

B. 个人区域网满足自身附近 10m 范围内移动数字终端设备联网的需求

C. IEEE 802.15.4 标准主要考虑低速无线个人区域网的应用

D. 蓝牙技术与 ZigBee 技术不属于 WPAN 的范畴

1-3-9 以下关于无线人体区域网 WBAN 基本概念的描述中，错误的是________。

A. 物联网智能医疗、环境智能、军事等应用推动了无线人体区域网 WBAN 的发展

B. 智能医疗应用系统不需要有很多节点，节点之间的距离一般在 1m 左右

C. 智能医疗应用系统对传输速率要求不高

D. 802.15.4 是 WBAN 的协议标准

1.4 计算机网络的组成与结构

1-4-1 以下关于 ISP 概念的描述中，错误的是________。

A. 大型 ISP 运营商要向 Internet 管理机构申请大量的 IP 地址

B. 用户需要通过 ISP 接入到 Internet

C. 最顶层的 ISP 称为 Tier-1 ISP

D. ISP 等级需要向 IETF 申请

1-4-2 以下关于第一层 ISP 特征的描述中，错误的是________。

A. 通过路由器组直接与其他第一层 ISP 连接，形成 Internet 的主干网

B. 与大量的第二层的 ISP 和其他网络连接
C. 与大量的本地 ISP 网络连接
D. 覆盖世界范围

1-4-3 以下关于 Internet 交换点 IXP 概念的描述中,错误的是________。
A. IXP 网络是由第一级 ISP 组建的
B. IXP 网络直接与第一层 ISP 网络连接
C. IXP 网络直接与区域 ISP、接入 ISP 网络连接
D. IXP 网络直接与内容提供商 ICP 的网络连接

1-4-4 以下关于 Internet 核心交换与边缘部分的抽象方法描述中,错误的是________。
A. Internet 系统可以看作是由边缘部分与核心交换部分两部分组成
B. 核心交换部分包括由大量路由器互联的服务器集群
C. 核心交换部分为应用程序进程通信提供服务
D. 网络应用程序运行在端系统

1.5 计算机网络的拓扑构型

1-5-1 以下关于网络拓扑概念的描述中,错误的是________。
A. 拓扑学是研究将实体抽象成的"点""线""面"之间的关系
B. 拓扑设计对网络性能、系统可靠性与通信费用都有重大影响
C. 计算机网络拓扑反映出网中节点与通信线路之间的关系
D. 计算机网络拓扑是指资源子网主机之间的结构

1-5-2 以下关于不同网络拓扑特点的描述中,错误的是________。
A. 星形拓扑网络的中心节点是网络性能与可靠性的瓶颈
B. 总线型拓扑网络必须解决多节点访问共享总线的介质访问控制策略问题
C. 环形拓扑网络的优点在于它不存在多节点访问环路的介质访问控制策略问题
D. 网状拓扑网络必须解决路由选择算法、流量控制与拥塞控制问题

1.6 分组交换技术的基本概念

1-6-1 以下关于数据交换方式的描述中,错误的是________。
A. 数据报是分组交换技术中的一种
B. 数据报方式适用于长报文、会话式通信
C. 数据报方式中每个中间节点独立地进行路由选择
D. 同一报文的不同分组可能要经过不同的传输路径通过通信子网

1-6-2 以下关于虚电路交换方式特点的描述中,错误的是________。
A. 虚电路方式在分组发送前,在发送方和接收方需要建立一条逻辑连接的虚电路
B. 虚电路工作过程分为虚电路建立阶段、数据传输阶段与虚电路拆除阶段
C. 通过虚电路传送的分组需要带有目的节点的地址
D. 每个节点可以同时在多个节点之间建立虚电路

1-6-3 以下关于网络延时概念的描述中,错误的是________。
A. 网络延时是指一个分组从源主机发出到达目的主机所需要经历的时间

B. 网络延时包括处理延时、排队延时、发送延时与传播延时

C. 一个分组通过同一条虚电路传输时，网络延时数值不变

D. 网络延时决定着分布式进程通信的质量

1-6-4 以下关于不同延时特点的描述中，错误的是________。

A. 路由器节点处理延时的大小取决于路由器计算能力与通信协议的类型

B. 路由器节点排队延时的大小取决于队列长度与端口发送速率

C. 一个端口发送延时的大小取决于端口发送速率

D. 传播延时的大小取决于传输介质的长度

1-6-5 计算和比较不同情况下的发送延时与传播延迟。

条件：发送节点与接收节点之间传输介质的长度 $D=100$km。电磁波在传输介质上的传播速度为 2×10^8 m/s。

(1) 数据长度为 1×10^7 bit，数据发送速率为 1Mbps。

(2) 数据长度为 1×10^3 bit，数据发送速率为 10Gbps。

1-6-6 已知：源节点与目的节点的距离为 20km，信号在线路中的传播速度为 200km/ms，一个分组的长度等于 1KB，并且数据发送延时与往返传播延时相等。求：数据发送速率为多少？

1-6-7 已知：① 分组数据长度为 P 位，分组头长度为 H 位。

② 源节点到目的节点之间的链路数为 h，每条链路上的传播延时为 D。

③ 数据传输速率为 B(bps)。

④ 电路连接建立的时间为 S(s)。

求解：通过线路交换传送总长度为 L 位的数据需要多少时间？

1-6-8 已知：① 待传输的报文长度为 L(b)。

② 从源主机到目的主机要经过 k 条线路。

③ 每一条线路的传播延时为 d(s)。

④ 数据传输速率为 b(bps)。

⑤ 在电路交换中，电路的建立时间为 s(s)。

⑥ 交换机排队等待时间忽略不计。

求：长度为 L 位的报文通过电路交换网传输的总延时。

1-6-9 已知：① 待传输的报文长度为 L(b)。

② 分组数据长度为 p，报头长度为 h，分组长度为$(p+h)$(b)。

③ 数据传输速率为 b(bps)。

④ 从源主机到目的主机要经过 k 条线路。

⑤ 路由器排队等待时间与每一条线路的传播延时忽略不计。

求：长度为 L 位的报文通过分组交换网传输的总延时。

***1-6-10** 在一个分组交换网中，假设：

① 报文长度为 L。

② 分组长度为 $p+h$，其中 p 为分组中数据字段的长度，h 为分组头长度。

③ 忽略传播延时与节点排队等待延时。

求：如果希望总的延时达到最小，那么分组中数据字段长度 p 应取多少？

1-6-11 以下关于面向连接服务与无连接服务的描述中,错误的是________。

A. 通信服务可以分为面向连接服务与无连接服务

B. 面向连接服务的数据传输过程必须经过连接建立、维护与释放三个阶段

C. 无连接服务中的每个分组都携带完整的目的节点地址,各个分组独立传送

D. 各层的网络协议不涉及面向连接服务与无连接服务的问题

1-6-12 以下关于连接、无连接服务与确认、不确认关系的描述中,正确的是________。

A. 无连接服务一定不采用确认与重传机制

B. 面向连接服务一定要采用确认与重传机制

C. 对应面向连接、确认与重传机制的网络通信协议最复杂

D. 计算机网络的传输层不会采用不可靠的无连接服务、不确认与重传的协议

1.7 网络体系结构与网络协议

1-7-1 以下关于网络体系结构概念的描述中,错误的是________。

A. 对于复杂的网络协议最好的组织方法是层次结构模型

B. 网络体系结构是网络协议的集合

C. 网络体系结构对网络要实现的功能进行了精确定义

D. 体系结构是抽象的,实现技术是实际的

1-7-2 以下关于网络协议概念的描述中,错误的是________。

A. 网络协议由语义、语法与时序三个要素组成

B. 语义定义数据分组与帧的结构

C. 语法定义用户数据与控制信息的结构与格式

D. 时序给出对事件实现顺序的详细说明

1-7-3 以下关于网络接口概念的描述中,错误的是________。

A. 接口是通信节点之间交换信息的连接点

B. 协议对接口信息交互过程与格式有明确的规定

C. 低层通过接口向高层提供服务

D. 只要接口条件不变,低层功能的具体实现方法不会影响整个系统的工作

1-7-4 以下关于OSI参考模型概念的描述中,错误的是________。

A. 定义了开放系统的层次结构、层次之间的相互关系,以及各层所包括的服务

B. “开放”是指遵循OSI标准的任何计算机之间都可以相互通信

C. 采用三级抽象:体系结构、服务定义与协议规范

D. 定义了协议软件编程方法

1-7-5 以下关于OSI参考模型层次划分原则的描述中,错误的是________。

A. 网中各主机都具有相同的层次

B. 不同主机的同等层具有相同的功能

C. 同一主机内相邻层之间通过接口通信

D. 不同主机的相邻层通过协议来实现同等层之间的通信

1-7-6 以下关于OSI参考模型的描述中,错误的是________。

A. 物理层为组成帧的二进制比特流传输提供服务

B. 数据链路层使得原始的物理线路成为无差错的数据链路
C. 网络层实现路由选择、分组转发、流量与拥塞控制等功能
D. 应用层为分布式进程通信之间提供点对点数据传输服务

1-7-7 以下不包括在 OSI 环境中的是________。
A. 应用层　　B. 应用进程　　C. 路由器　　D. 传输层

1-7-8 以下关于 OSI 环境中数据传输的过程的描述中，错误的是________。
A. 应用层为数据(data)加上报头组成应用层协议数据单元
B. 传输层协议数据单元被称为数据报或分组(packet)
C. 数据链路层协议数据单元被称为帧(frame)
D. 物理层传输的是比特

1-7-9 长度为 200B 的应用层数据，在传输层加上 20B 的 TCP 报头，在网络层加上 20B 的分组头，在数据链路层有加上 18B 的 Ethernet 帧头与帧尾，那么传输效率是________。
A. 75.0%　　B. 76.5%　　C. 77.5%　　D. 78.0%

1-7-10 以下关于 TCP/IP 协议特点的描述中，错误的是________。
A. 独立于特定的计算机硬件与操作系统
B. 独立于特定的网络硬件，适用于网络的互联
C. 全部采用地址转换 NAT 方法来处理 IP 地址
D. 标准化的应用层协议，可以提供多种可靠的网络服务

1-7-11 以下关于 TCP/IP 参考模型层次结构的描述中，错误的是________。
A. TCP/IP 参考模型的应用层与 OSI 参考模型的应用层、表示层、会话层相对应
B. TCP/IP 参考模型的传输层与 OSI 参考模型的传输层相对应
C. TCP/IP 参考模型的互联层与 OSI 参考模型的网络层相对应
D. TCP/IP 参考模型的主机-网络层与 OSI 参考模型的数据链路层相对应

1-7-12 以下 TCP/IP 层次中，没有规定具体协议的是________。
A. 主机-网络层　　B. 网络层　　C. 传输层　　D. 应用层

1-7-13 以下关于 RFC 文档特点的描述中，错误的是________。
A. Internet 标准的制定需要经过“草案、建议标准、草案标准、标准”阶段
B. “草案”阶段的文档是提供给大家讨论用的
C. “建议标准”是某项标准研究当前实验的进展报告
D. “标准”阶段的 RFC 文档表示该文档已经成为 Internet 协议标准

第二部分　同步练习答案与解析

1.1　计算机网络的形成与发展

1-1-1 分析：ARPANET 在计算机网络发展的历史上起到了十分重要的作用。设计该例题的目的是考查读者对计算机网络技术发展历史以及对 ARPANET、网络应用、TCP/IP 协议关系的理解。

(1) 美国军方在 20 世纪 60 年代初期开始了 ARPANET 的研究。

(2) ARPANET是计算机网络技术发展中的一个里程碑,它的研究成果对促进网络技术发展和理论体系的研究产生重要作用,同时也证实分组交换概念的正确性。ARPANET为后来出现的Internet的形成与发展奠定了基础。

(3) 1983年,TCP/IP协议成为ARPANET的协议标准。

(4) DNS、E-mail、FTP、TELNET作为ARPANET重要的网络应用,推动了计算机网络技术的发展。Web是20世纪90年代出现的技术。

因此,C的描述是错误的。

答案:C。

1-1-2 分析:设计该例题的目的是加深读者对计算机网络与Internet特征的认识。这里涉及对以下技术的评价。

(1) 计算机网络是计算机技术与通信技术高度发展、密切结合的产物。

(2) 从计算机网络的发展过程看,分组交换概念与技术的确为计算机网络的发展奠定了理论基础。

(3) OSI参考模型对推动计算机网络理论与协议标准化的发展起到了重要的推动作用,它的层次性网络体系结构的思想与模型现在已广泛应用,但是构建Internet的核心协议应该是TCP/IP协议体系。

(4) Web技术与应用对于Internet应用的发展确实起到了重要的推动作用。

因此,C的描述是错误的。

答案:C。

1-1-3 分析:设计该例题的目的是加深读者对移动互联网特点的认识。这里涉及以下几个问题。

(1) 移动IP与无线通信技术研究为移动互联网发展奠定了坚实基础,这一点是正确的。

(2) 移动通信属于电信行业,移动通信网最初设计的目标是为用户在移动过程中的语音通话提供服务。电信业看到互联网广阔的应用前景,逐步向互联网应用扩展,将移动通信网语音业务与互联网业务的融合,为移动互联网开辟了广阔的发展空间。

(3) 从目前的应用趋势看,智能手机、可穿戴计算等智能终端设备成为计算机之外,在移动互联网应用中发展最快的接入设备,并且正在推动移动互联网应用的快速发展。

(4) 无线自组网与无线传感器网络是移动通信一类特殊的应用,不是移动互联网应用的基本模式。

因此,D的描述是错误的。

答案:D。

1-1-4 分析:设计该例题的目的是加深读者对物联网特点的认识。

(1) 在研究物联网发展背景时,人们发现现实物理世界与网络虚拟世界融合的需求,是促进物联网概念形成与研究发展的重要原因之一。

(2) 感知、智能与通信是支撑信息技术发展的三大支柱,感知、智能与网络技术的融合为物联网的发展奠定了技术基础。

(3) 物联网应用包括智能工业、智能农业、智能交通、智能电网等,应用涉及各行各业,不同应用系统之间差别很大,因此物联网中的智能终端设备一定是多样化的,很多智能终端

设备都需要根据具体应用的需求，利用网络环境嵌入式系统的硬件、软件的开发技术进行专门的设计和开发。在智能手机基础上进行开发是一种方式，但是不可能都在智能手机的基础上进行开发。

(4) 物联网为计算机网络的接入技术、传输结束、分布式进程通信与网络安全技术研究提出了很多研究课题。

因此，C 的描述是错误的。

答案：C。

1-1-5 分析：设计这道习题的目的是帮助读者对计算机网络发展趋势的理解。

(1) 计算机网络正在沿着“互联网—移动互联网—物联网”的轨迹，“由小到大”地发展、壮大；“由表及里”地渗透到社会的各个角落。

(2) 计算机网络遵循着“互联网＋”的模式，在与各行各业的跨界融合中，推动着我国国民经济发展方式的转型与社会发展。

(3) 如果说互联网的作用是扩大了信息社会人与人之间信息共享的广度，移动互联网的作用是扩大了信息共享的深度与灵活性，那么物联网利用传感器、无线传感器网络与射频标签 RFID 等感知技术，将人与人的互联，扩大到人与物、物与物的互联，使人类对外部世界具有“更全面的感知能力、更广泛的互联互通能力、更智慧的处理能力”。

因此，D 的描述是错误的。

答案：D。

1.2 计算机网络技术发展的三条主线

1-2-1 分析：计算机网络技术的发展可以归纳成三条主线。设计该例题的目的是加深读者对第一条主线 ARPANET-TCP/IP-Internet 的认识。在讨论 Internet 技术的发展时，需要注意以下几个重要的特点：

(1) 在从 ARPANET 演变到 Internet 的过程中，广域网、城域网与局域网技术的研究与应用得到了快速发展；广域网、城域网与局域网技术的成熟与标准化，又加快了 Internet 的发展进程。

(2) ARPANET 的研究促进了 Internet 的发展，TCP/IP 协议体系是 ARPANET 与 Internet 的核心技术，而 IEEE 802 模型是局域网协议体系。

(3) 计算机网络、电信网络与有线电视网络的三网融合趋势已经十分清晰。

(4) 与传统的客户/服务器(C/S)工作模式不同，对等(P2P)工作模式淡化了服务提供者与服务使用者的界限，进一步扩大了网络资源共享范围和深度。

因此，A 的描述是错误的。

答案：A。

1-2-2 分析：设计该例题的目的是加深读者对第二条主线无线网络技术发展的认识。在讨论无线网络技术发展时，需要注意以下几个重要的特点：

(1) 无线网络可以分为两类：基于基础设施与无基础设施。

(2) IEEE 802.11 无线局域网可以有两类组网方式：一种是需要有基站-接入点 AP 的基于基础设施的无线局域网，如常见的家庭无线局域网与办公室无线局域网；另一类是不需要事先设立基站的无线自组网 Ad hoc 的组网方式。

(3) IEEE 802.16 协议解决的是无线城域网问题,主要用于大楼与大楼之间的点对点无线通信问题,为大楼与大楼内部的有线或无线局域网互联提供技术支持,因此 IEEE 802.16 无线城域网是需要事先建立基站的,属于基于基础设施的无线网络。

(4) 无线传感器网络是无线自组网与传感器技术的结合。无线网状网是无线自组网在接入领域的一种应用。

因此,C 的描述是错误的。

答案:C。

1-2-3 分析:设计这道习题的目的是加深读者对第三条主线网络安全技术特点的理解。

在讨论网络安全技术时,需要注意以下几个重要的特点:

(1) 随着互联网广泛应用于现代社会的政治、经济、文化、教育、科学研究与社会生活的各个领域,网络安全已经成为影响社会稳定与国家安全的重要因素之一。世界各国将"网络空间"上升为与一个国家"海、陆、空、太空"同等重要的第五个疆域,将"网络安全"上升到"网络空间安全"的高度去认识,纷纷制定"国家网络空间安全战略"。

(2) 目前网络攻击已经开始从当初出于显示才能等目的,逐步发展到出于经济利益驱动的有组织犯罪,甚至是恐怖活动。

(3) 从网络安全的角度,TCP/IP 协议本身存在着一定的漏洞,为网络攻击提供了攻击的可能性。网络安全研究的很多课题是围绕着这个问题开展的。

因此,C 的描述是错误的。

答案:C。

1-2-4 设计这道习题的目的是加深读者对网络安全特点的理解。

(1) 网络安全是一个系统的社会工程。网络安全的研究是一个涉及技术、管理、道德与法制环境等多个方面的问题。

(2) 网络的安全性是一个链条,它的可靠程度取决于链条中最薄弱的环节。

(3) 人们在加强网络安全与网络管理技术研究的同时,必须加快网络法制建设,加强人们的网络安全意识、网络法制观念与道德教育。

因此,B 的描述是错误的。

答案:B。

1.3 计算机网络定义与分类

1-3-1 分析:设计该例题的目的是加深读者对计算机网络定义内涵的理解。在讨论网络定义时,需要注意以下几个主要问题:

(1) 计算机网络可以定义为"以能够相互共享资源的方式互联起来的自治计算机系统的集合"。

(2) 组建计算机网络的主要目的是实现联网计算机资源的共享。计算机资源主要指计算机的硬件、软件与数据资源。网络用户不但可以使用本地计算机资源,而且可以通过网络访问远程计算机的资源,可以调用网中多台计算机协同完成一项任务。网络资源不限于计算机的硬件资源。

(3) 计算机网络由多个互联的主机组成,主机之间要做到有条不紊地交换数据,每个主

机都必须遵守一些事先规定好的通信规则。这就和人们之间的对话一样,如果人与人之间要顺畅地交流,就需要大家都说同样的语言(中文或英文)。如果一个说中文,而一个说英文,这时就需要找一个翻译参与才能实现对话。

因此,B的描述是错误的。

答案:B。

1-3-2 分析:设计该例题的目的是加深读者对按传输技术进行网络分类方法的理解。在讨论网络分类时,需要注意以下几个重要的特点:

(1) 按照所采用的传输技术,网络也可以分为以下两类:广播式网络与点对点式网络。

(2) 在广播式网络中,所有联网计算机都共享一个公共通信信道。当一台计算机利用共享通信信道发送一个分组时,所有其他的计算机都只能处于接收状态。

(3) 在点对点式网络中,每条物理线路连接一对计算机。假如两台计算机之间没有直接连接的线路,那么它们之间的分组传输就要通过中间节点转发。采用分组存储转发与路由选择机制是点对点式网络与广播式网络的重要区别之一。

因此,D将广播式网络中的“介质访问控制”取代了“路由选择”机制,从而造成了混淆。应该明确:点对点式网络的主要特征是“存储转发”与“路由选择”。

答案:D。

1-3-3 分析:

(1) 网络互联(internet,internetworking)是表述“将多个计算机网络互联成大型网络系统的技术”的术语。internet与internetworking术语的含义是相同的。

(2) “Internet是internet中的一种”的提法是正确的。但是不能说“internet也是Internet中的一种”。因为Internet(或因特网、互联网)是专用名词,专指目前广泛应用、覆盖了全世界、提供Web等服务的大型网际网。

(3) 随着Internet的广泛应用,一些大型企业、管理机构也采用了Internet的组网方法,采用TCP/IP协议与Web的系统设计方法,将分布在不同地理位置的部门局域网互联成企业内部的专用网络系统,供内部员工办公使用,不连接或不直接连接到Internet,这种内部的专用网络系统叫做Intranet。

因此,C的描述是错误的。

答案:C。

1-3-4 分析:计算机网络的分类方法有多种,其中最主要的方法是根据覆盖范围进行分类的方法。其中,按计算机网络覆盖的地理范围进行分类,是一种常用的方法,它可以很好地反映不同类型网络的技术特征。

(1) 过去按覆盖的地理范围划分,计算机网络可分为以下4类:广域网、城域网、局域网与个人区域网。物联网技术的发展,尤其是智能医疗应用的发展,催生了人体区域网技术与标准的发展。因此可以分为5类:广域网、城域网、局域网、个人区域网与人体区域网。

(2) 按照覆盖距离从小到大排列:连接人体周边1m范围内可穿戴与可植入的传感器的无线网络称为无线人体区域网(WBAN);连接用户计算机身边10m之内计算机、打印机、PDA与智能手机等数字终端设备的无线网络称为无线个人区域网(WPAN);覆盖10m~10km的网络称为局域网(LAN);覆盖10~100km的网络称为城域网(MAN);覆盖100~

1000km的网络称为广域网(WAN)。

(3) 接入网是指能够帮助用户计算机或智能终端设备接入到Internet的网络,它可以是WBAN或WPAN,可以是有线或无线的LAN网,也可以利用电话交换网、电视传输网或电力线接入。因此,接入网是指网络的一种用途,不属于按覆盖的地理范围划分的计算机网络类型,一般不将它作为一种类型的计算机网络来对待。

因此,D的描述是错误的。

答案:D。

1-3-5 分析:设计该例题的目的是加深读者对广域网特点的理解。在讨论广域网特点时,需要注意以下几个主要的问题:

(1) 广域网是一种公共数据网络。

局域网、个人区域网、人体区域网一般属于一个单位或个人所有,组建成本低、易于建立与维护,通常是自建、自管、自用。而广域网建设投资很大,管理困难,通常由电信运营商负责组建、运营与维护。有特殊需要的国家部门与大型企业也可以组建自己使用和管理的专用广域网。网络运营商组建的广域网为广大用户提供高质量的数据传输服务,因此这类广域网属于公共数据网络(Public Data Network,PDN)的性质。用户可以在公共数据网络上开发各种网络服务系统。如果用户要使用广域网服务,需要向广域网的运营商租用通信线路或其他资源。网络运营商需要按照合同的要求,为用户提供电信级7×24(每个星期7天、每天24小时)的服务。

(2) 广域网路由器的一侧作为城市的宽带出口,通过光纤链路与相邻城市的路由器连接。更多的广域网的互联可以形成大型的网际网,从而构成Internet的主干网。

(3) 广域网路由器的另一侧与城域网、城市的有线与无线的电信网络以及城市电视传输网互联。用户通过城域网与广域网互联的网际网接入到Internet。

(4) 大量的广域网互联形成了Internet的宽带、核心交换平台,从而构成了层次结构的大型互联网络。广域网研究的重点放在“如何提供保证服务质量(Quality of Service,QoS)的宽带核心交换技术”上,而不是接入技术。保证接入用户范围Internet的服务质量的责任由城域网承担。

因此,C关于广域网研究重点的描述是错误的。

答案:C。

1-3-6 分析:设计这道例题的目的是帮助读者深入了解宽带城域网的特点。宽带城域网技术的主要特征表现在以下几个方面:

(1) 如果说广域网设计的重点是保证大量用户共享主干通信链路的容量,那么城域网设计的重点不完全在链路,而是交换节点的性能与容量。城域网的每个交换节点都要保证大量接入用户的服务质量。

(2) 宽带城域网结构是由“三个平台与一个出口”,即管理平台、业务平台、网络平台以及城市宽带出口构成。

(3) 宽带城域网的业务平台可以为用户提供Internet接入业务、虚拟专网业务、话音业务、视频与多媒体业务、内容提供业务等。

(4) 传统电信、有线电视与计算机网络在IP业务的融合成为了宽带城域网的核心业务,也体现出“三网融合”的发展趋势。

因此，A 关于宽带城域网是电信、有线电视与计算机网络在 IP 业务上融合的描述是错误的。

答案：A。

1-3-7 分析：设计这道例题的目的是帮助读者深入了解局域网的特点。局域网技术的主要特征表现在以下几个方面：

(1) 局域网覆盖有限的地理范围，它适用于机关、校园、工厂等有限范围内的计算机、终端与各类信息处理设备联网的需求。

(2) 局域网可以用于办公室、家庭个人计算机的接入，园区、企业与学校的主干网络，以及大型服务器集群、存储区域网络、云计算服务器集群的后端网络。

(3) 局域网能够提供高数据传输速率(10Mbps～100Gbps)、低误码率的高质量数据传输环境。

(4) 当前最流行的局域网是有线局域网 Ethernet 与无线局域网 Wi-Fi。

因此，C 关于局域网最高传输速率的数据是错误的。

答案：C。

1-3-8 分析：设计这道例题的目的是帮助读者深入了解无线个人区域网 WPAN 的特点。WPAN 技术的主要特征表现在以下几个方面：

(1) 个人区域网络(PAN)主要是用无线通信技术实现联网设备之间的通信，因此出现了无线个人区域网络(WPAN)的概念。

(2) 随着笔记本计算机、智能手机、PDA、投影仪与信息家电的广泛应用，人们逐渐提出了自身附近 10m 范围内的个人操作空间(POS)移动数字终端设备联网的需求。

(3) IEEE 802.15 工作组致力于无线个人区域网的标准化工作，它的任务组 TG4 制定 IEEE 802.15.4 标准，主要考虑低速无线个人区域网络(LR-WPAN)应用问题。

(4) 蓝牙技术与 ZigBee 技术属于 WPAN 的范畴。

因此，D 关于蓝牙技术与 ZigBee 技术的描述是错误的。

答案：D。

1-3-9 分析：设计这道例题的目的是帮助读者深入了解无线人体区域网 WBAN 的特点与标准问题。回答这个问题需要注意以下几点：

(1) 作为近距离无线通信，虽然已经存在无线个人区域网(WPAN)的概念，但是智能医疗应用有它的特殊性。疾病监控与健康保健系统需要将人体携带的传感器或移植到人体内的生物传感器节点组成人体区域网，将采集的人体生理信号(如温度、血糖、血压、心跳等参数)，以及人体活动或动作信号、人所在的环境信息，通过无线方式传送到附近的基站。物联网智能医疗等应用推动了 WBAN 的发展。

(2) WBAN 的研究目标是希望为健康医疗监控应用提供一个集成硬件、软件的无线通信平台，特别强调要适应可穿戴与可植入的生物传感器的尺寸，以及低功耗的无线通信要求。

(3) 随着物联网智能医疗应用的迅速发展，IEEE 于 2007 年 11 月成立了专门致力于为医疗保健服务的 802.15 工作组(IEEETG6)，研究适用于人体与人体周边无线通信的无线人体区域网络 WBAN 的通信技术及标准。经过 5 年多的努力，于 2012 年 3 月公布了 802.15.6 标准的正式版本。

(4) IEEE 802.15.6 标准具有短距离、低功耗、低成本、实时性与安全性高的特点,除了可以应用于智能医疗之外,还可以应用于航空、个人娱乐、体育运动、环境智能、军事与社会公共安全等领域。

因此,D 关于 IEEE 802.15.4 标准的描述是错误的。

答案:D。

1.4 计算机网络的组成与结构

1-4-1 分析:设计这道例题的目的是帮助读者深入了解 ISP 的结构与运行机制。回答这个问题需要注意以下几点:

(1) 从网络结构的角度来看,Internet 是一个结构复杂,并且在不断变化的网际网。Internet 并不是由任何一个国家组织或国际组织来运营,而是由一些私营公司分别运营各自的部分。

(2) 用户接入与使用各种网络服务都需要由 ISP 来提供。

(3) ISP 可以分为最顶层的第一层 ISP、第二层的区域或国家级的 ISP,以及第三层的 ISP。

(4) 最顶层的 ISP 数量很少,被称为 Tier-1 ISP。

(5) 大型 ISP 运营商向 Internet 管理机构申请了大量的 IP 地址,铺设了大量的通信线路,购置了高性能路由器与服务器。

(6) 只要家庭用户或企业用户向 ISP 提出申请并交纳一定的费用,ISP 就会为用户以动态或静态的方式提供 IP 地址和接入服务。小的 ISP 运营商可以向电信公司租用通信线路来提供接入服务。

(7) 实际上,没有一个组织来正式批准哪些 ISP 属于第一层,但是从它的三个特征(规模、连接位置与覆盖范围),可以确定这些 ISP 是否处于第一层 ISP 的位置。第一层 ISP 的特点是:通过路由器组直接与其他第一层 ISP 连接,形成 Internet 的主干网;与大量的第二层的 ISP 和其他网络连接;覆盖世界区域。

因此,D 关于 ISP 等级资格的描述是错误的。

答案:D。

1-4-2 分析:设计这道例题的目的是帮助读者深入了解第一层 ISP 的特征。回答这个问题需要注意以下几点:

最顶层的 ISP 数量很少,被称为 Tier-1 ISP。1994 年美国出现了第一层的 ISP,它们是 Sprint、MCI、AT&T、Qwest 等。实际上,没有一个组织来正式批准哪些 ISP 属于第一层,但是从它的三个特征(规模、连接位置与覆盖范围),可以确定这些 ISP 是否处于第一层 ISP 的位置。第一层 ISP 的特征是:

- 通过路由器组直接与其他第一层 ISP 连接,形成 Internet 的主干网。
- 与大量的第二层的 ISP 和其他网络连接。
- 覆盖世界区域。

因此,C 关于第一级 ISP 与大量的本地 ISP 网络连接的描述是错误的。

答案:C。

1-4-3 分析:为了提高分组转发速度,ISP 通过一个或多个路由器组,与其他同层、高

层或低层 ISP 网络连接。随着 Internet 用户规模的扩大与网络流量的剧增，为了更加降低分组转发延迟与成本，出现了由第三方组建的 Internet 交换点 IXP 网络，直接与第一层 ISP、区域 ISP、接入 ISP，以及内容提供商 ICP 的网络连接。

因此，A 关于 IXP 网络是由第一级 ISP 组建的描述是错误的。

答案：A。

1-4-4 分析：设计这道例题的目的是帮助读者深入了解 Internet 核心交换部分与边缘部分的抽象方法。回答这个问题需要注意以下几点：

（1）面对复杂的 Internet 结构，研究者必须对复杂网络进行简化和抽象，而将 Internet 系统分为边缘部分与核心交换部分是最有效的方法之一。

（2）Internet 系统由边缘部分与核心交换部分两部分组成。网络应用程序运行在边缘部分，核心交换部分为应用程序进程通信提供服务。

（3）Internet 核心交换部分包括由大量路由器互联的广域网、城域网和局域网。

（4）边缘部分利用核心交换部分所提供的数据传输服务功能，使得接入 Internet 的主机之间能够相互通信和共享资源。

（5）边缘部分的用户设备也称为端系统（end system）。端系统是指能够运行 FTP 应用程序、E-mail 应用程序、Web 应用程序、P2P 文件共享的 Napster 应用程序、Skype 即时通信应用程序的计算机和各种数字终端设备。因此，端系统又被统称为主机。

因此，B 关于核心部分组成的描述是错误的。

答案：B。

1.5 计算机网络的拓扑构型

1-5-1 分析：网络拓扑是研究网络结构与组成的重要方法。不同的网络，其网络拓扑结构也可能是不一样的。设计该例题的目的是加深读者对网络拓扑概念和拓扑分类的理解。在讨论网络拓扑时，需要注意以下几个重要的特点：

（1）拓扑学是将实体抽象成与其大小、形状无关的“点”，将连接实体的线路抽象成“线”，进而研究“点”“线”“面”之间的关系。

（2）计算机网络拓扑是通过网络中节点与通信线路之间的几何关系表示网络结构，反映出网络各实体间的结构关系。

（3）拓扑设计是计算机网络设计的第一步，它对网络性能、系统可靠性与通信费用都有重大影响。

（4）计算机网络拓扑是指通信子网的拓扑构型。

从以上的总结中可以看出，通信子网承担着为资源子网中的计算机提供分组传输服务的功能，它决定了网络性能、系统可靠性与通信费用。研究计算机网络拓扑主要就是研究通信子网的拓扑构型问题。

因此，D 的描述是错误的。

答案：D。

1-5-2 分析：设计该例题的目的是加深读者对网络拓扑特点与分析的理解。在讨论网络拓扑时，需要注意以下几个重要的特点：

（1）基本的网络拓扑可以分为 5 种基本类型：星形、环形、总线型、树形与网状。

(2) 星形拓扑网络的节点通过点对点通信线路与中心节点连接。中心节点控制全网的通信。星形拓扑构型结构简单,易于实现,便于管理。但是,网络的中心节点是全网性能与可靠性的瓶颈,中心节点的故障可能造成网络瘫痪。

(3) 环形拓扑网络中节点通过点对点通信线路连接成闭合环路。环中数据将沿一个方向逐站传送。环形拓扑结构简单,传输延时确定,但是环中每个节点与连接节点之间的通信线路都会成为网络可靠性的瓶颈。令牌是控制环形网络中节点如何有效地利用共享环路传输分组的介质访问控制方法,同时环形网络还需要为节点接入、退出和环的维护制定控制策略。

(4) 总线型拓扑网络中所有的节点都连接在一条作为公共传输介质的总线上。如果有两个或两个以上的节点同时打算利用公共总线发送数据时,就会出现冲突,造成传输失败。总线型拓扑结构的优点是结构简单,缺点是必须解决多节点访问总线的介质访问控制策略问题。

(5) 树形拓扑网络中节点按层次进行连接,信息交换主要在上、下节点之间进行,相邻及同层节点之间一般不进行数据交换或数据交换量比较小。树形拓扑可以看成是星形拓扑的一种扩展,树形拓扑网络适用于汇集信息的应用要求。

(6) 网状拓扑中节点之间的连接是任意的,没有规律。网状拓扑的主要优点是系统可靠性高。但是,网状拓扑结构复杂,必须采用路由选择算法、流量控制与拥塞控制方法。

综上所述,无论是总线型拓扑或环形拓扑都需要解决节点接入和退出网络问题,只是不同的拓扑解决的方法不同而已。典型的采用总线型拓扑的 Ethernet 采用的是随机访问控制的 CSMA/CD 方法,而典型的环形网络采用的是令牌控制方法。

因此,C 关于环形拓扑的特点的描述是错误的。

答案:C。

1.6 分组交换技术的基本概念

1-6-1 分析:设计该例题的目的是加深读者对数据报交换方式的理解。在讨论数据报交换方式时,需要注意以下几个问题。

(1) 分组交换方式可以分为两类:数据报(DG)与虚电路(VC)。

(2) 在数据报交换方式中,分组传输前不需要预先在源主机与目的主机之间建立"线路连接"。源主机发送的每个分组经过中间节点转发时,转发节点通过路由选择算法为每一个分组选择一条传输路径。

(3) 数据报交换方式主要有以下几个特点:

- 同一报文的不同分组可以经过不同的传输路径通过通信子网。
- 同一报文的不同分组到达目的节点时可能出现乱序、重复与丢失现象。
- 每个分组在传输过程中都必须带有目的地址与源地址。
- 数据报方式的传输延迟较大,适用于计算机的突发性通信,不适用于长报文、会话式通信。

因此,B 对数据报交换方式特点的描述是错误的。

答案:B。

1-6-2 分析:设计该例题的目的是加深读者对虚电路交换方式特点的理解。讨论虚电

路交换方式的特点涉及以下几个问题：

（1）虚电路方式试图将数据报与线路交换相结合起来，发挥这两种方法各自的优点，以达到最佳的数据交换效果。

（2）数据报方式在分组发送前，发送方与接收方之间不需要预先建立连接。虚电路方式在分组发送前，发送方和接收方需要建立一条逻辑连接的虚电路。

（3）虚电路方式的工作过程分为三个阶段：虚电路建立阶段、数据传输阶段与虚电路拆除阶段。

（4）虚电路方式主要有以下几个特点：

- 在每次分组传输之前，需要在源节点与目的节点之间建立一条逻辑连接。由于连接源节点与目的节点的物理链路已经存在，因此不需要真正去建立一条物理链路。
- 一次通信的所有分组都通过虚电路顺序传送，因此分组不必带目的地址、源地址等信息。分组到达目的节点时不会出现丢失、重复与乱序的现象。
- 分组通过虚电路上的每个节点时，节点只需要进行差错检测，而不需要进行路由选择。
- 通信子网中每个节点可以与多个节点建立多条虚电路连接。

（5）虚电路方式与线路交换方式的区别是：

- 虚电路是在传输分组时建立的逻辑连接，之所以称之为“虚电路”，是因为这种电路不是专用的。
- 每个节点可以同时在多个节点之间建立虚电路，每条虚电路支持这两个节点之间的数据传输。
- 用数据报方式传输的每个分组都要带有源地址与目的地址。用虚电路方式传输时不需要在每个分组中都带上源地址与目的地址。

（6）由于虚电路方式具有分组交换与线路交换的优点，因此在计算机网络中得到广泛的应用。

答案：C。

1-6-3　分析：分组交换网延时是指一个分组从源主机发出，经过分组交换网（或链路）的传输，到达目的主机所需要的时间，因此分组交换网延时也统称为“网络延时”。

分组交换网为联网主机的进程通信提供服务，数据通过分组交换网的延时决定着分布式进程通信的质量，并直接影响网络应用软件与应用系统的性能，因此网络延时是描述网络性能的重要指标之一。

在理想状态下，源主机（或路由器）发送的数据分组能够瞬间通过分组交换网到达目的主机，没有延时，也不存在分组丢失与传输出错。显然这是不可能的。源主机发出的分组经过传输路径上每个路由器转发时，都会产生不同类型的延时，这些延时主要有：

- 处理延时（processing delay）。
- 排队延时（queuing delay）。
- 发送延时（transmission delay）。
- 传播延时（propagation delay）。

分组在网络中产生的总延时（total nodal delay）等于以上四种延时的总和。由于网络延时的大小牵涉到主机、路由器与链路的状态，其过程非常复杂，即使同一个报文的不同分

组通过同一条虚电路传输时,也不肯定它的传输延时不变。因此,C的表述是错误的。

答案:C。

1-6-4 分析:

(1) 处理延时:一个路由器节点处理延时的大小取决于路由器计算能力以及通信协议的复杂度。

(2) 排队延时:一个路由器节点排队延时的长短取决于队列长度与端口发送速率。

(3) 发送延时:当分组长度不变时,发送延时的大小取决于端口发送速率。

(4) 传播延时:电磁波在空间中的传播速度是一定的。分组传播延时的大小取决于的传输介质的长度。

因此,C的描述不全面。

答案:C。

1-6-5 分析:发送延时、传播延时是两个容易混淆的概念,本题设计的目的是加深读者的这两个重要的概念的理解。

(1) 发送延时。

节点发送延时=发送的比特数/发送速率=N/S。

(2) 传播延时。

传播延时=D/V。

计算:

(1) 发送延时:$T_{t1}=1\times10^7/1\times10^6=10(\text{s})$

传播延时:$T_{c1}=1\times10^5/2\times10^8=50\times10^{-3}(\text{s})=50(\text{ms})$

(2) 发送延时:$T_{t2}=1\times10^3/1\times10^{10}=1\times10^{-7}(\text{s})=0.1(\mu\text{s})$

传播延时:$T_{c2}=1\times10^5/2\times10^8=5\times10^{-3}(\text{s})=5(\text{ms})$

答案:

(1) 当数据长度为1×10^7b,数据发送速率为1Mbps时,发送延时为10s,传播延时为50ms。

(2) 当数据长度为1×10^3b,数据发送速率为1Gbps时,发送延时为0.1μs,传播延时为50ms。

1-6-6 分析:这是一道涉及数据传输中传播延时、发送延时关系的习题,目的是加深读者对这两个概念的理解。解决这个问题的困难是将线路距离、信号传播速度、传播延时、往返传播延时,以及分组长度、发送速率之间建立起关系。

(1) 线路距离除以信号传播速度等于传播延时,传播延时的2倍等于往返传播延时。

(2) 分组长度除以发送速率(或传输速率)等于发送延时。

计算:

(1) 往返传播延时 $T1=2D/V=(2\times20\times10^3)/2\times10^8=2\times10^{-4}(\text{s})$

(2) 假设发送速率为S,分组长度为$L=1024\times8(\text{b})$

那么,发送延时 $T2=(1024\times8)/S$

(3) 已知 $T1=T2$,即$(1024\times8)/S=2\times10^{-4}$,可得 $S=40.96(\text{Mbps})$。

答案:发送速率等于40.96Mbps。

(注意:在计算二进制字节长度时1KB=1024B,但是在计算速率的时候使用的是十进

制，因此 1kbps=1000bps≠1024bps；同样，40.98×106 bps=40.98Mbps≠40Mbps。这是计算机与通信两个领域中所采用的二进制与十进制的区别引起的误解，也是初学者经常出现的错误。）

1-6-7 分析：设计这道习题的目的是帮助读者进一步理解线路交换的特点。

（1）线路交换的过程如图 1-1 所示。

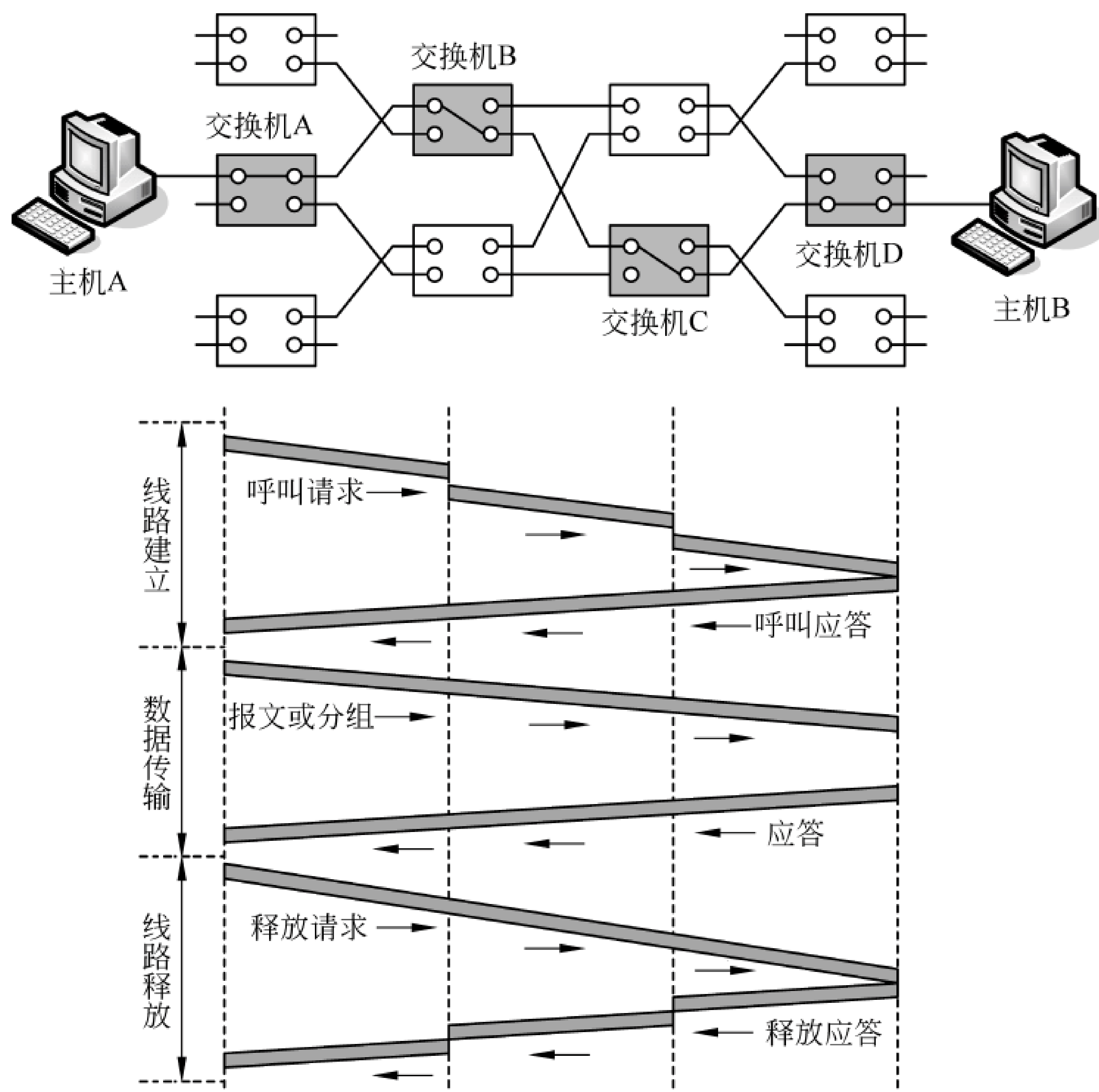


图 1-1 线路交换的过程示意图

线路交换时间的组成包括：

- 线路建立延时。
- 发送节点发送多帧的总发送延时。
- 帧通过每一段链路传播延时与通过多段链路总传播延时。

（2）计算。

① 线路建立延时为 S。

② 一个分组的长度 $=P+H$，发送一帧的发送延时为 $(P+H)/B$。

数据总长度为 L，需要分为 L/P 帧（已知 L 是 P 的整数倍）。

那么发送这些帧总共的发送延时为 $(P+H)L/PB$。

③ 每段链路传播延时为 D，N 段链路总的传播延时为 DN。

假设：传输过程中不出错，不考虑确认和释放线路连接的时间。通过数据交换网传输送长度为 L 的数据，总共需要的时间是：$T=S+(P+H)L/PB+DN$。

答案：通过数据交换网传输送长度为 L 的数据，总共需要的时间为

$$T = S + (P + H)L/PB + DN$$

1-6-8 分析：设计这道习题的目的是加深读者对线路交换网工作原理的理解。

电路交换过程的总延时组成如图1-2所示。

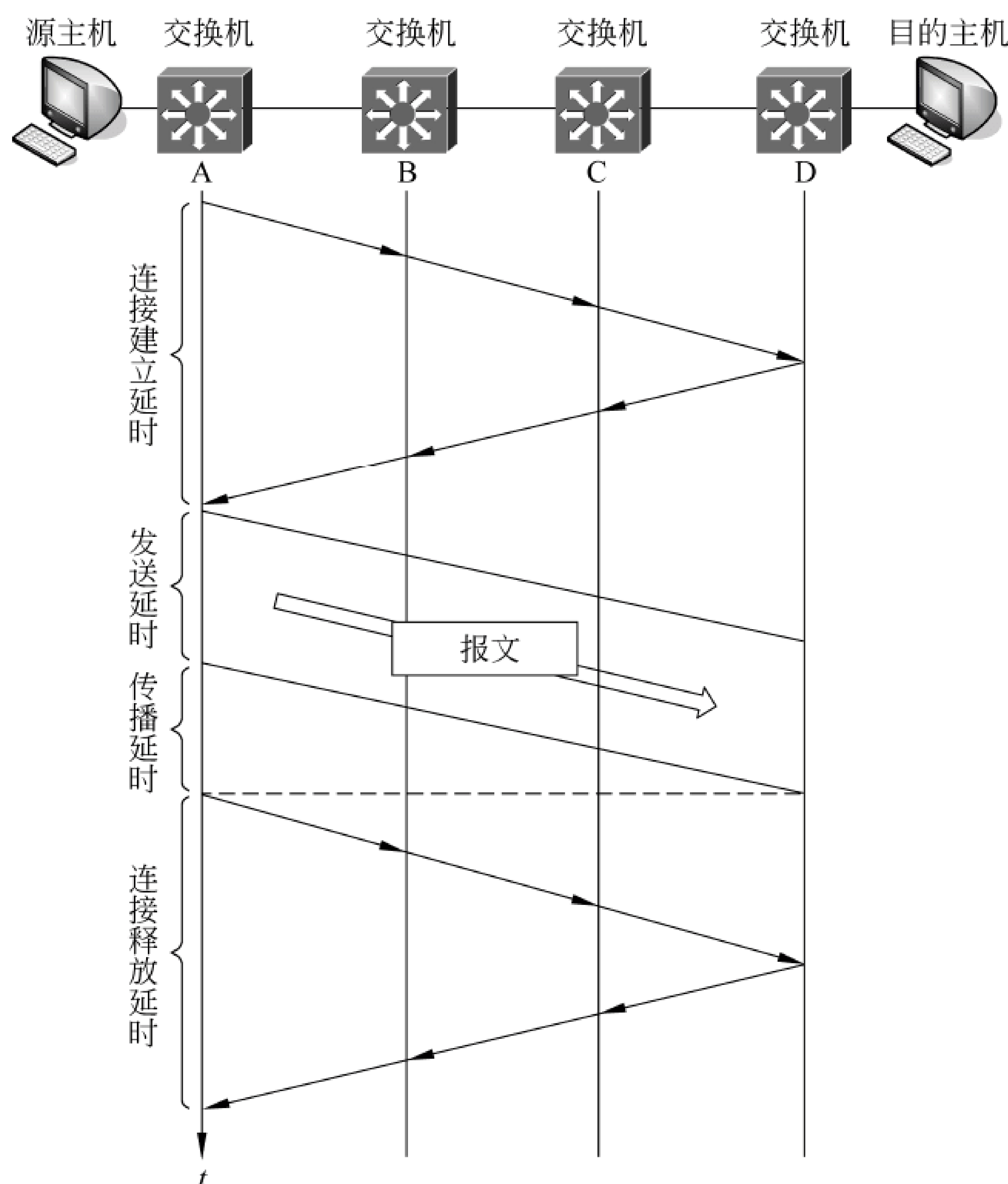


图1-2 电路交换过程的总延时组成

忽略排队等待时间，那么电路交换总延时为

$$T1 = 连接建立延时 + 发送延时 + 传播延时 + 连接释放延时$$

(1) 假设连接建立与释放都是由源主机发起，并且连接建立延时＝连接释放延时＝S(秒)。

(2) 由于传送的报文长度为L(b)，数据传输速率为B(bps)，那么报文的发送延时等于L/B(秒)。

(3) 由于每条线路的传播延时为D(秒)，共有k段线路，因此电路交换的传播延时等于$D\times k$(秒)。

那么，电路交换总延时 $T = 2S+L/B+Dk$。

答案：长度为L报文通过电路交换网传输的总延时等于$2S+L/B+Dk$。

1-6-9 分析：设计这道习题的目的是加深读者对分组交换网工作原理的理解。

(1) 将长度为L的报文分为长度为p的分组，可以分为$n=L/p$个分组。

(2) 已知数据传输速率为b(bps)，分组长度应该是数据长度加上报头长度，即为$(p+h)$b。那么主机发送一个分组的发送延时是$\Delta t=(p+h)/b$(秒)。

(3) 主机发送 n 个分组的发送延时 $=n\times\Delta t=((p+h)/b)\times(L/p)$。

(4) 已知从源主机到目的主机要经过 k 条线路,每个分组需要通过 $(k-1)$ 个路由器转发,那么发送延时 $=(k-1)\times(p+h)/b$。

(5) 由于每条线路的传播延时为 d(秒),共有 k 段线路,因此分组交换的传播延时等于 $d\times k$(s)。

(6) 分组交换总延时 $T2$ = 发送延时 + 传播延时,即

$$T2=((p+h)/b)\times(L/p)+(k-1)\times(p+h)/b$$

答案:长度为 L 报文通过分组交换网传输的总延时等于 $((p+h)/b)\times(L/p)+(k-1)\times(p+h)/b$。

*1-6-10 分析:在分组交换中,协议效率与分组头长度以及分组的数据长度相关。设计本例题的目的是加深读者对影响分组交换网延时的因素、计算方法的理解。

(1) 分组结构如图 1-3 所示。

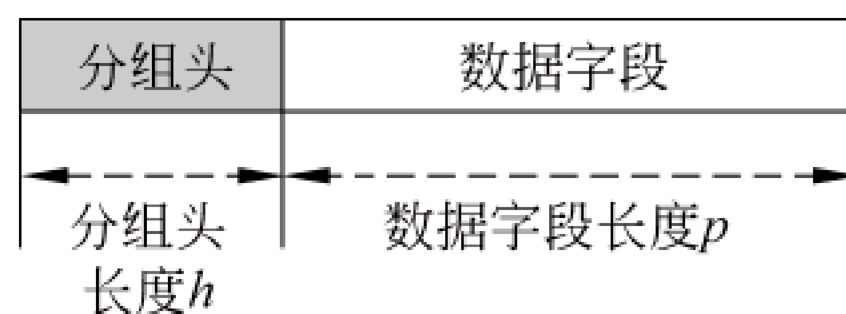


图 1-3 分组结构示意图

(2) 已知条件:

① 报文长度为 L;

② 分组长度为 $p+h$,其中 p 为分组中数据字段的长度,h 为分组头长度;

③ 从源节点到目的节点要经过 k 条电路;

④ 数据传输速率为 b(bps)。

⑤ 忽略传播延时与节点排队等待延时。

(3) 参考计算分组延时公式,做出以下修改:

① 忽略传播延时,即 $d=0$;

② 用 $L=p+h$;

③ 如果将一个长度为 L 的报文分为长度为 p 的分组,那么可以分为 $n=L/p$ 个。

④ 已知数据传输速率为 b(bps),考虑到分组头长度,分组长度为 $p+h$,那么一个节点发送一个分组的发送延时是 $\Delta t=(p+h)/b$(秒)。发送 n 个分组的发送延时 $=n\times\Delta t=(p+h)/b\times(L/p)$。

⑤ 已知从源节点到目的节点要经过 k 条电路,每个分组需要通过 $k-1$ 个节点转发,那么发送延时 $=(k-1)\times(p+h)/b$。

分组传输总延时:

$$T=(p+h)/b\times(L/p)+(k-1)\times(p+h)/b \tag{1-1}$$

计算:分组传输总延时如式(1-1)所示,本题求使分组传输总延时 T 达到最小时的分组数据字段长度 p 值。

$$T'(p)=-(Lh/bp^2)+(k-1)/b$$

令 $T'(p)=0$,即:

$$-(Lh/bp^2)+(k-1)/b=0 \tag{1-2}$$

$$p=(Lh/(k-1))^{1/2}$$

答案:当 $p=(Lh/(k-1))^{1/2}$ 时,分组传输总延时 T 达到最小。

1-6-11 分析：设计这道习题的目的是加深读者对网络中通信服务与通信协议的面向连接服务与无连接服务的理解。

(1) 数据通信分为面向连接服务与无连接服务两类。

面向连接服务和电话系统的工作模式类似。无连接服务与邮政系统服务的信件投递过程类似。两者的区别是：

① 面向连接服务的数据传输过程必须经过连接建立、连接维护与释放连接的三个阶段；无连接服务数据传输过程不需要经过连接建立、连接维护与释放连接三个阶段。

② 在面向连接服务的数据传输过程中，各个分组不需要携带目的节点的地址；在无连接服务中，每个分组都要携带完整的目的节点地址。

③ 面向连接服务的传输连接类似一个通信管道，发送者在一端放入数据，接收者从另一端取出数据。面向连接数据传输的数据收发顺序不变；无连接服务发送的分组可能经历不同路径发送到目的主机，接收的分组可能出现乱序、重复与丢失现象。

④ 面向连接服务的传输的可靠性好，但是协议复杂，通信效率不高；无连接服务的可靠性不是很好，但是通信协议相对简单，通信效率比较高。

(2) 面向连接服务与无连接服务对实现服务的协议复杂性有很大影响。根据主机对数据传输效率和可靠性要求的不同，设计者可以选择面向连接服务服务或无连接服务。

(3) 在网络数据传输的各层(例如物理层、数据链路层、网络层与传输层)都会涉及面向连接服务与无连接服务的问题。物理层、数据链路层、网络层与传输层的通信方式与协议的制定方面都需要事先确定：是采用面向连接的服务，还是无连接服务。采用的通信服务类型不同，通信的可靠性与协议的复杂性也不相同。

因此，D 的描述是错误的。

答案：D。

1-6-12 分析：设计这道习题的目的是加深读者对网络中通信服务与通信协议的面向连接、无连接，以及确认、不确认关系的理解。

(1) 从数据传输与网络协议的角度来看，面向连接服务、无连接服务与确认、不确认机制之间并没有必然的联系。

(2) 面向连接服务可以要求采用确认和重传机制，提供最为可靠的数据传输服务；面向连接服务也可以不要求采用确认机制，数据传输的可靠性主要由面向连接服务来保证。

(3) 无连接服务也可以要求采用确认和重传机制，由确认和重传机制来提高数据传输的可靠性；无连接服务也可以采用不确认机制，但是数据传输的可靠性较低。

(4) 在网络的各个层次的通信协议设计中，人们可以在面向连接与确认服务、面向连接与不确认服务、无连接与确认服务、无连接与不确认服务四种情况中，根据不同的通信要求选择不同的服务类型。

(5) 实际上，由于无连接服务也可以采用不确认机制的协议，因此计算机网络的传输层 UDP 协议采用的就是无连接服务、不确认的机制。UDP 协议提供的是“尽力而为”的传输服务。

因此，D 的描述是正确的。

答案：D。

1.7 网络体系结构与网络协议

1-7-1 分析：设计该例题的目的是加深读者对网络体系结构概念的理解。“网络体系结构”是计算机网络中一个基本和重要的概念。在理解网络体系结构时，需要注意以下几个重要问题：

(1) 网络体系结构是网络层次结构模型与各层协议的集合。网络体系结构对计算机网络应该实现的功能进行了精确定义，而这些功能是用什么样的硬件与软件去完成的，则是具体的实现问题。网络体系结构是抽象的，而实现技术是具体的，它是指能够运行的硬件和软件。

(2) 各层之间相对独立，高层只需要知道下层能够提供的服务，而不需要知道低层的服务是如何实现的。

(3) 各层可以采用最合适的技术来实现，各层实现方法和技术的改变不影响其他层次。

(4) 每层的功能与所提供的服务都已有精确的说明，因此这有利于促进协议的标准化。

综上所述，B将网络体系结构描述为“网络协议的集合”，忽略了一个重要的概念“层次结构模型”，严格地描述应该是：“网络体系结构是网络层次结构模型与各层协议的集合”。因此，B的描述是错误的。

答案：B。

1-7-2 分析：设计该例题的目的是加深读者对网络协议概念的理解。在讨论网络协议概念时，需要注意以下几个主要问题：

(1) 计算机网络中多个互联的计算机之间要有条不紊地交换数据，每台计算机都必须遵守一些事先约定好的网络协议。

(2) 网络协议主要由三要素(语义、语法与时序)组成。

(3) 语法定义了用户数据与控制信息的结构与格式。

(4) 语义定义了需要发出何种控制信息，以及需要完成的动作与响应。

(5) 时序对事件实现顺序进行了详细的说明。

因此，B对语义的描述是错误的。

答案：B。

1-7-3 分析：设计该例题的目的是加深读者对“接口”概念的理解。在讨论“接口”概念时，需要注意以下几个主要问题：

(1) 接口是同一节点内相邻层之间交换信息的连接点。

(2) 协议对接口信息的交互过程与格式有明确的规定。

(3) 低层通过接口向高层提供服务。

(4) 只要接口条件与功能不变，低层功能的具体实现方法不会影响整个系统的工作。

综上所述，接口是同一节点内相邻层之间交换信息的连接点，而不是通信节点之间交换信息的连接点。因此，A的描述是错误的。

答案：A。

1-7-4 分析：设计该例题的目的是加深读者对OSI参考模型概念的理解。在讨论OSI参考模型概念时，需要注意以下几个重要问题：

(1) OSI参考模型中的“开放”是指只要遵循OSI标准，一台计算机就可以与位于世界

上任何地方、遵循同一标准的其他计算机进行通信。

(2) OSI参考模型定义了开放系统的层次结构、层次之间的相互关系,以及各层所包含的服务。它作为一个框架来协调和组织各层协议的制定,也是对网络内部结构最精炼的概括与描述。

(3) OSI的服务定义详细地说明了各层所提供的服务。系统所能够提供的服务功能与具体实现功能的技术无关。

(4) OSI参考模型只是描述了一些概念,用来协调进程间通信标准的制定,并没有定义具体的实现方法。

(5) OSI参考模型并不是一个标准,而是一个在制定标准时所使用的概念性的框架。

(6) OSI标准中采用的是三级抽象:体系结构、服务定义与协议规范。

综上所述,OSI参考模型是一个在制定标准时所使用的概念性的框架,与具体实现功能的技术无关。因此,C的描述是错误的。

答案:C。

1-7-5 分析:OSI参考模型将整个通信功能划分为七个层次,其层次划分的主要原则是:

(1) 网络中各主机都具有相同的层次。

(2) 不同主机的同等层具有相同的功能。

(3) 同一主机内相邻层之间通过接口通信。

(4) 每层可以使用下层提供的服务,并向其上层提供服务。

(5) 不同主机的同等层通过协议来实现同等层之间的通信。

因此,D对OSI参考模型层次划分原则的描述是错误的。

答案:D。

1-7-6 分析:设计该例题的目的是加深读者对OSI参考模型各层的主要功能的理解。在讨论参考模型各层的主要功能时,需要注意以下几个问题:

(1) 物理层的主要功能是利用传输介质实现比特序列的传输。

(2) 数据链路层主要功能是采用差错控制与流量控制方法,使得有差错的物理线路变成无差错的数据链路。

(3) 网络层主要功能是实现路由选择、分组转发、流量与拥塞控制。

(4) 传输层主要功能是向高层用户提供可靠的"端-端"(end-to-end)通信服务,并且对高层屏蔽了下层数据通信的具体细节。

(5) 会话层主要功能是负责维护两台通信计算机之间的进程通信,以便确保"点-点"(point-to-point)传输不中断,以及管理数据交换等。

(6) 表示层主要功能是用于处理两个通信的计算机系统交换数据的表示方式,完成数据的格式变换、数据的加密与解密、数据的压缩与恢复等。

(7) 应用层主要功能是为应用软件提供多种网络服务,如文件服务、数据库服务、电子邮件与其他网络服务。

因此,D对物理层功能的描述是错误的。

答案:D。

1-7-7 分析:设计该例题的目的是加深读者对OSI环境概念的理解。在讨论OSI环

境概念时，需要注意以下几个问题：

(1) OSI 环境包括主机的应用层到物理层的七层，以及通信子网。

(2) 连接主机的物理传输介质不包括在 OSI 环境中。

(3) 应用进程不包括在 OSI 环境中。

因此，应用进程不包括在 OSI 环境中。

答案：B。

1-7-8 分析：设计该例题的目的是加深读者对 OSI 环境中数据流特点的理解。在讨论 OSI 环境中的数据流时，需要注意以下几个主要问题：

(1) 当应用进程 A 的数据传送到应用层时，应用层为数据(data)加上应用层报头组成应用层协议数据单元，然后再传送到表示层。

(2) 表示层接收到应用层协议数据单元后，加上表示层报头组成表示层的协议数据单元，再传送到会话层。

(3) 会话层接收到表示层协议数据单元后，加上会话层报头组成会话层协议数据单元，再传送到传输层。

(4) 传输层接收到会话层协议数据单元后，加上传输层报头构成了传输层的协议数据单元，传输层协议数据单元被称为报文(message)。

(5) 网络层协议数据单元被称为分组(packet)。

(6) 数据链路层协议数据单元被称为帧(frame)。

(7) 物理层协议数据单元是比特(bit)。

选项 B 混淆了传输层与网络层的协议数据单元。

答案：B。

1-7-9 分析：设计该例题的目的是加深读者对通信协议对传输效率影响的理解。

长度为 200B 的应用层数据，在传输层加上 20B 的 TCP 报头，在网络层加上 20B 的分组头，在数据链路层又加上 18B 的 Ethernet 帧头与帧尾，那么传输效率是：

$$200 \div (200+20+20+18) = 200 \div 258 \approx 77.5\%$$

因此，C 的数值是正确的。

答案：C。

1-7-10 分析：设计该例题的目的是加深读者对 TCP/IP 协议特点的理解。在讨论 TCP/IP 协议特点时，需要注意以下几个主要特点：

(1) 开放的协议标准。

(2) 独立于特定的计算机硬件与操作系统。

(3) 独立于特定的网络硬件，可以运行在局域网、城域网与广域网之上，适用于网络的互联。

(4) 统一的网络地址分配方案，使得所有的 TCP/IP 设备都具有唯一的网络地址。

(5) 标准化的应用层协议，可以提供多种可靠的网络服务。

因此，C 的描述是错误的。

答案：C。

1-7-11 分析：设计该例题的目的是加深读者对 TCP/IP 参考模型的层次结构特点的理解。在讨论 TCP/IP 参考模型的层次结构特点时，需要注意以下几个主要问题：

(1) TCP/IP 参考模型只定义了应用层、传输层、互联层与主机-网络层。

(2) TCP/IP参考模型的应用层与OSI参考模型的应用层、表示层、会话层相对应。
(3) TCP/IP参考模型的传输层与OSI参考模型的传输层相对应。
(4) TCP/IP参考模型的互联层与OSI参考模型的网络层相对应。
(5) TCP/IP参考模型的主机-网络层与OSI参考模型的数据链路层、物理层相对应。
因此,D的描述是错误的。
答案:D。

1-7-12 分析:设计这道习题的目的是加深读者对TCP/IP层次特点的理解。回答这个问题需要注意以下几点:

(1) 主机-网络层是TCP/IP参考模型的最低层,它负责通过网络发送和接收IP分组。TCP/IP对主机-网络层并没有规定具体的协议,它允许使用广域网、局域网与城域网的各种协议。
(2) 互联网络层使用的是IP协议。
(3) 传输层定义了TCP协议与UDP协议。
(4) 应用层是TCP/IP参考模型中的最高层。应用层包括各种标准的网络应用协议,并且总是不断有新的协议加入。TCP/IP应用层的基本协议主要有TELNET、FTP、SMTP、HTTP、DNS、SNMP与DHCP等。
答案:A。

1-7-13 分析:设计这道习题的目的是帮助读者加深对请求评价文档特点的理解。回答这个问题需要注意以下几点:

(1) RFC(Request For Comment)文档是网络技术研究人员获取技术资料的重要来源之一。Internet标准的制定需要经过四个阶段:草案、建议标准、草案标准、标准。
(2) "草案"阶段的文档是提供给大家讨论用的。
(3) 当研究人员提交的文档经过IETF专家审查认为有可能成为协议标准时,将被接受为"建议标准"阶段的RFC文档。
(4) 处于"草案标准"阶段的RFC文档,表示该文档正在按协议标准的要求进行审查。
(5) 处于"标准"阶段的RFC文档表示该文档已经成为Internet协议标准。
(6) RFC文档有三种形式:实验性文档、信息性文档与历史性文档。

- 实验性RFC文档表示该文档是某项技术研究当前实验的进展报告。
- 信息性RFC文档表示该文档是与Internet相关的一般性信息或指导性的信息。
- 历史性RFC文档表示该协议已经被新的协议取代,或者是从未使用的标准。

显然,C的描述是错误的。
答案:C。

第三部分 综合练习——术语解析

从给出的26个定义中挑出20个,并将标识定义的字母填在对应术语前的空格位置。

(1) ________ Intranet
(2) ________ WSN
(3) ________ packet switching
(4) ________ OSI RM
(5) ________ end system
(6) ________ Internet

(7) ________ network topology
(8) ________ Ad hoc
(9) ________ ISP
(10) ________ protocol stack
(11) ________ IoT
(12) ________ computer network
(13) ________ WBAN
(14) ________ RFC
(15) ________ distributed network
(16) ________ WAN
(17) ________ network architecture
(18) ________ IANA
(19) ________ virtual circuit
(20) ________ IETF

A. 国际标准化组织制定的网络参考模型。
B. 将报文划分成格式固定的分组的交换方式。
C. 覆盖全世界、最重要的网际网。
D. 互联网技术人员之间发布技术研究进展与标准的一类文档。
E. 以能够相互共享资源的方式互联起来的自治计算机系统的集合。
F. 一种自组织、对等式、多跳、无线移动网络。
G. 为用户提供接入 Internet 服务的企业。
H. 保证网络中计算机能有条不紊地交换数据的一系列的规则。
I. 覆盖一个国家、地区,或横跨几个洲的远程计算机网络。
J. 将几十公里范围内的大量企业、机关、公司的局域网互联起来的网络。
K. 没有中心交换节点的网状结构网络。
L. 采用 TCP/IP 协议与 Web 的系统设计方法的企业内部的专用网络。
M. 将无线自组网与传感器技术结合起来的网络。
N. 将多个计算机网络互联成大型网络系统的技术。
O. 网络层次结构模型与各层协议的集合。
P. Internet 边缘部分的数字终端设备。
Q. 以服务器为中心的工作模式。
R. 组织、监督 IP 地址的分配、MAC 地址中的公司标识等编码的注册管理工作部门。
S. 需要通过交换机交换的通信方式。
T. 实现人与人、人与物、物与物之间互联的网络。
U. 连接用户 1m 之内的终端设备联网的无线通信网络。
V. 主机中从应用层到物理层的七层以及通信子网,但不包括传输介质。
W. 基于节点与通信线路之间的几何关系的网络结构表示方式。
X. 分组传输前不需要预先在源主机与目的主机之间建立线路连接的交换方式。
Y. 在分组发送前,发送方和接收方需要建立一条逻辑连接的电路。
Z. Internet 协会 ISOC 的执行机构。

参考答案:

(1) L	(2) M	(3) B	(4) A	(5) P
(6) C	(7) W	(8) F	(9) G	(10) H
(11) T	(12) E	(13) U	(14) D	(15) K
(16) I	(17) O	(18) R	(19) Y	(20) Z

第 2 章 物理层

第一部分 同步练习

2.1 物理层与物理层协议的基本概念

2-1-1 以下关于物理层服务功能的描述中,错误的是________。

A. 物理层向数据链路层提供比特流传输服务

B. 物理层服务功能主要是:物理连接的建立、维护与释放,比特流的传输

C. 设置物理层就是要屏蔽传输介质、设备与通信技术的差异性

D. 数据传输的可靠性主要靠物理层来保证

2-1-2 以下关于传输介质与信号编码关系的描述中,错误的是________。

A. 连接物理层的传输介质可以有不同类型

B. 通信线路分为两类:点对点通信线路和广播通信线路

C. 物理层根据所使用传输介质的不同制定相应的物理层协议

D. 物理层协议规定数据信号的编码方式、信号类型、传输速率与数据链路质量

2.2 数据通信的基本概念

2-2-1 以下关于信息、数据与信号的描述中,错误的是________。

A. 信息的载体可以是文字、语音、图形或图像,以及它们的组合

B. ASCII 码是文字、语音信息变换成二进制代码的标准之一

C. 计算机网络中传输的是二进制代码的电信号

D. ASCII 码包括用于数据通信的控制字符

2-2-2 以下关于信号概念的描述中,错误的是________。

A. 传输介质与传输设备确定电信号的类型

B. 电平幅度连续变化的电信号称为模拟信号

C. 用脉冲信号不同的电平跳变来表示的电信号为数字信号

D. 模拟的语音信号不能够用于传输计算机网络中的二进制数字信号

2-2-3 以下关于同步技术的描述中,错误的是________。

A. 同步是要求通信双方在时间基准上保持一致的过程

B. 数据通信的同步包括位同步与字符同步

C. 位同步分为外同步法与内同步法

D. 异步通信的传输效率高

2-2-4 以下关于双绞线传输介质特点的描述中，错误的是________。

A. 双绞线是局域网中最常用的传输介质

B. 双绞线可以由一对或多对相互绝缘的铜导线组成

C. 每对导线相互绞合是为了使线路向外部辐射的电磁波达到最小

D. 高带宽的超5类线、6类以及7类双绞线可以用于高速局域网中

2-2-5 以下关于光纤结构特点的描述中，错误的是________。

A. 光纤的纤芯的直径为8～100μm

B. 超高纯度石英玻璃纤维制作的纤芯传输损耗最低

C. 光纤是由纤芯、外面包层与涂覆层组成的

D. 纤芯折射率低于外面的包层

2-2-6 以下关于光纤传输特点的描述中，错误的是________。

A. 传输速率高　　B. 双向传输　　C. 安全性好　　D. 误码率低

2-2-7 以下关于光纤物理层参数标准的描述中，错误的是________。

A. 传输模式　　B. UTP接口

C. 最大传输距离　　D. 上行光纤与下行光纤光载波的频率

2-2-8 以下关于光缆结构特点的描述中，错误的是________。

A. 光缆是由缆芯、中心加强芯与外部保护层组成

B. 护套使得光缆具有很好的抗拉、抗压能力

C. 中心加强芯用来加强光缆的抗拉强度

D. 缆芯包含一根高带宽的光纤

2-2-9 以下关于工业、科学与医药专用ISM频段的描述中，错误的是________。

A. 915MHz、2.4GHz与5.8GHz三个频段属于ISM频段

B. ISM频段属于免予申请的频段

C. 发射功率可以不受规定

D. Wi-Fi使用ISM频段

2-2-10 以下关于无线信号功率的描述中，错误的是________。

A. 信号功率单位是瓦(W)或毫瓦(mW)

B. IEEE 802.11协议中使用的是信号功率的相对值

C. 计算公式为 $dBm=10\times\log_2(P_{mW})$

D. －dBm表示信号强度小于1mW

2-2-11 主机A不能够接收到主机B无线信号的原因是________。

A. 主机B发送的信号频率为2.465GHz

B. 主机A接收机的频带为2.4500～2.4800GHz

C. 接收机A的接收灵敏度都为－60dBm

D. 接收机B接收到主机A的无线信号强度为－65dBm

2-2-12 以下关于微波通信特点的描述中，错误的是________。

A. 微波对应的信号波长为3～30m
B. 微波信号一般只能可视传播
C. 微波信号容易实现远距离通信
D. 微波一般采用点对点方式通信

2-2-13 以下关于蜂窝移动通信特点的描述中,错误的是________。
A. 每个小区中设立一个基站
B. 用户手机通过基站接入网中
C. 若干个小区构成的区群
D. 小区覆盖的半径一般为1～2km

2-2-14 以下关于卫星通信特点的描述中,错误的是________。
A. 通信距离远
B. 覆盖面积广
C. 不受地理条件限制
D. 费用与通信距离相关

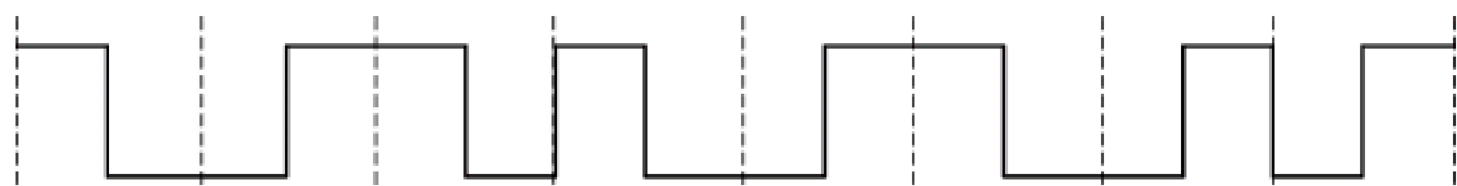
2.3 频带传输技术

2-3-1 以下关于模拟数据编码方法的描述中,错误的是________。
A. 具备调制与解调功能的模拟通信设备称为调制解调器
B. 移频键控FSK方法是通过改变载波信号角频率来表示数字信号1、0
C. 用相位的绝对值表示数字信号1、0,称为相对调相
D. 八相调制的每个码元表示4比特的数据

2-3-2 以下关于数字数据编码方法的描述中,错误的是________。
A. 基带传输是指基本不改变数字信号频带直接传输数字信号的方法
B. 非归零码必须用另一个信道同时传送同步信号
C. 曼彻斯特编码属于自含时钟编码方法
D. 差分曼彻斯特编码的时钟信号频率等于发送频率

2.4 基带传输技术

2-4-1 下图是一个8b的差分曼彻斯特编码信号的波形,它代表的数据是什么?



2-4-2 以下关于PCM编码方法的描述中,错误的是________。
A. PCM技术的典型应用是语音数字化
B. PCM工作包括采样、量化与编码
C. 取样频率f应取信道允许通过的信号最高频率的2倍
D. PCM用7位二进制数,采样速率为8000样本/秒,数据速率为64kbps

2-4-3 以下关于信道速率概念的描述中,错误的是________。
A. 奈奎斯特准则描述了无噪声状态下的“带宽”与“速率”的关系

B. 奈奎斯特准则表示最大传输速率在数值上是信道带宽的 2 倍
C. 香农定理描述了在有随机热噪声状态下的“带宽”与“速率”的关系
D. $S/N=30\text{dB}$ 表示信道上的信号功率是噪声功率的 30 倍

2-4-4 如果 $S/N=30\text{dB}$，带宽 $B=3000\text{Hz}$，根据香农定理，有限带宽、有热噪声信道的最大数据传输速率为多少？

2-4-5 在无噪声情况下，线路带宽为 3kHz，采用 4 相位、每个相位用 4 种振幅表示的 QAM 调制方式。线路的最大数据传输速率为多少？

2.5 多路复用技术

2-5-1 以下关于多路复用基本概念的描述中，错误的是________。
A. 时分多路复用通过为多个信道分配互不重叠的时间片来达到多路复用的目的
B. 频分多路复用通过设置多个频率互不重叠的信道来达到同时传输多路信号的目的
C. 波分多路复用通过光振幅调制达到多路复用的目的
D. 码分多址是在同一频段不同信道采用特殊挑选的码型达到互不产生干扰的目的

2-5-2 以下关于同步时分多路复用的描述中，错误的是________。
A. 时分多路复用可以分为同步时分多路复用与统计时分多路复用
B. 同步时分多路复用将时间片固定分配给多个信道
C. 统计时分多路复用允许动态地分配时间片
D. 时分多路复用中传输的“帧”就是数据链路层的“帧”

2-5-3 如果要在一条线路上设计一个频分多路复用系统，已知一条通信线路的带宽为 100kHz，每路信号带宽为 3.2kHz，相邻信道之间的隔离带宽为 0.8kHz。那么这条信道可以传输多少路信号？

2.6 同步光纤网 SONET 与同步数字体系 SDH

2-6-1 以下关于基本速率标准的描述中，错误的是________。
A. T1 载波速率是针对脉冲编码调制 PCM 的时分多路复用 TDM 设计的
B. T1 载波速率是 1.544Mbps
C. E1 载波速率是 2.048Mbps
D. STM-1 速率是 51.84Mbps

2-6-2 以下关于 SDH 速率体系基本概念的描述中，错误的是________。
A. SDH 定义了三种速率：SONET 的 STS、OC 速率标准、SDH 的 STM 标准
B. OC 定义的是光纤上传输的光信号速率
C. SONET 定义的电信号速率标准是以 T1 为基础的
D. 对应于 STS-1 的是第 1 级 OC-1

2.7 接入技术

2-7-1 以下关于接入技术基本概念的描述中，错误的是________。
A. 接入技术关系到用户能得到的网络服务的类型、服务质量与资费等问题

B. 接入可以分为家庭接入、校园接入、机关与企业接入

C. 宽带接入主要有 ADSL 技术、HFC 技术、光纤、无线接入技术

D. 无线接入主要是靠蓝牙技术

2-7-2 以下关于 xDSL 的描述中,错误的是________。

A. 数字用户线(DSL)是利用一对电话线同时实现通话与上网的技术方案

B. ADSL 在电话线上提供带宽不对称的上下行通道

C. G. Life 标准又称为“轻量级 ADLS 标准”

D. ADSL2+标准上行速率可以达到 16Mbps

2-7-3 以下关于 HFC 接入技术的描述中,错误的是________。

A. HFC 技术的本质是用光纤取代有线电视网络中的干线同轴电缆

B. 小区内部接入用户家庭使用同轴电缆,形成光纤与同轴电缆混合使用的传输网络

C. HFC 形成以头端为中心的网状结构

D. 从头端向用户传输的信道称为下行信道

2-7-4 以下关于光纤接入技术的描述中,错误的是________。

A. 光纤接入是指局端与用户端之间完全以光纤作为传输介质的接入方式

B. 光纤接入可以分为有源光网络接入与无源光网络接入

C. 家庭与办公室接入主要采用有源光网络接入方式

D. FTTx 的 x 表示不同的光纤接入地点

2-7-5 以下关于不同光纤接入技术特点的描述中,错误的是________。

A. FTTH 省去了铜馈线、配线与引入线,增加了带宽,减少了网络维护工作量

B. FTTB 采用光纤到楼、高速局域网到户,是一种经济和实用的接入方式

C. FTTO 与 FTTC 的区别主要在于 DSLAM 部署的位置与覆盖的用户数

D. FTTC 是一种基于优化 xDSL 技术的宽带接入方式

2-7-6 以下关于无源光网络 PON 特点的描述中,错误的是________。

A. 无源光网络 PON 是一种点对多点的系统

B. 无源光接入网 ODN 典型的拓扑是网状结构

C. 目前发展最快的是 PON 与 Ethernet 相结合的 EPOS 技术

D. IEEE 制定了下行速率提高到 10Gbps 的 802.3av 10Gbps EPON 标准

2-7-7 在 CDMA 系统中,两个站的码片序列分别为:

A:(−1+1−1+1+1+1−1−1)

B:(−1−1+1−1+1+1+1−1)

现在接收到码片序列为 S:(−1+1−3+1−1−3+1+1)。

请判断:是哪个站发送的数据?发送的二进制数是 0 还是 1?

2-7-8 以下关于移动通信接入技术的描述中,错误的是________。

A. 移动通信的主要概念包括接口、信道、移动台与基站

B. 无线通信中手机与基站通信的接口称为空中接口

C. 基站与手机之间的通信是通过空中接口实现的

D. 3G/4G/5G 研究的是移动通信的网络结构

第二部分　同步练习答案与解析

2.1　物理层与物理层协议的基本概念

2-1-1　分析：设计该例题的目的是加深读者对物理层的服务功能的理解。在讨论物理层的服务功能时，需要注意以下几个主要问题：

（1）由于网络使用的传输介质与设备种类繁多，各种通信技术存在着很大的差异，并且各种新的通信技术又在快速发展。这些差异使数据链路层只需要考虑本层的服务与协议，而不需要考虑网络具体使用哪些传输介质与设备。

（2）物理层处于网络参考模型的最低层，它向数据链路层提供比特流传输服务。数据链路实体通过与物理层的接口将数据比特流传送给物理层；物理层将比特流按照传输介质的需要进行编码；然后将信号通过传输介质传输到下一个节点的物理层。物理层服务功能主要是：物理连接的建立、维护与释放，比特流的传输。

（3）物理层的主要功能是向数据链路层提供比特流传输服务，物理层对于比特流的传输可靠性可以采取一定的保障措施，但主要还是依靠数据链路层、网络层与传输层共同协作实现的。因此，D的描述是错误的。

答案：D。

2-1-2　分析：设计该例题的目的是加深读者对传输介质与信号编码关系的理解。在讨论传输介质与信号编码的关系时，需要注意以下几个主要问题：

（1）连接物理层的传输介质可以有不同类型，如电话线、同轴电缆、光纤与无线通信线路。

（2）不同类型的传输介质对于被传输的信号要求也不同。例如，电话线路只能用于传输模拟语音信号，不能够直接传输计算机产生的二进制数字信号。如果要求通过电话线路传输数字信号，那么在发送端就要将数字信号变换成模拟信号，再通过电话线路传输；在接收端将接收到的模拟信号还原成数字信号。

（3）如果希望通过光纤来传输数字信号，那么发送端也需要将电信号变换为光信号；接收端再将光信号还原成电信号。

（4）由于计算机网络使用的通信线路分为两类：点-点通信线路和广播通信线路。点-点通信线路用于连接通信的两个节点；而广播通信线路的一条公共通信线路可以连接多个节点。需要注意的是，广播通信线路可以分为有线与无线两种。因此，物理层协议可以分为两类：基于点-点通信线路的物理层协议与基于广播通信线路的物理层协议。

（5）物理层的一个重要功能是：根据所使用传输介质的不同，制定相应的物理层协议，规定数据信号的编码方式、传输速率以及相关的通信参数。

物理层协议不涉及数据链路质量的问题。因此，D关于物理层协议基本内容的描述是错误的。

答案：D。

2.2　数据通信的基本概念

2-2-1　分析：设计该例题的目的是加深读者对信息、数据与信号关系的理解。在讨论

信息、数据与信号关系时,需要注意以下几个主要问题:

(1) 在数据通信技术中,信息、数据与信号是很重要的概念,它们分别涉及通信的三个不同层次的问题。

(2) 通信的目的是交换信息,信息的载体可以是文字、语音、图形或图像。

(3) 计算机产生的信息一般是字母、数字、语音、图形或图像的组合。为了传送这些信息,首先要将字母、数字、语音、图形或图像用二进制代码来表示。

(4) 在网络中,为了传输二进制代码的数据,必须将它们用模拟或数字信号编码的方式表示。数据通信是指在不同计算机之间传输表示字母、数字、语音、图形或图像的二进制代码0、1比特序列的模拟或数字电信号的过程。

(5) ASCII码本是一个信息交换编码的国家标准,但是后来被国际标准化组织ISO接受,成为国际标准ISO 646,又称为国际5号码。因此,它被用于计算机内码,也是数据通信中的编码标准。

需要注意的是,ASCII码采用7个二进制位编码,可以表示128个字符。字符分为图形字符与控制字符两类。图形字符包括数字、字母、运算符号、商用符号等。例如,数字5的ASCII编码为0110101、字母A的ASCII编码为1000001。控制字符用于数据通信收发双方动作的协调与信息格式的表示。例如,控制字符"发送结束EOT"的ASCII编码为0000100。ASCII码不能解决语音信号的编码问题。

因此,B的描述是不正确的。

答案:B。

2-2-2 分析:设计该例题的目的是加深读者对信号的基本概念的理解。在讨论信号概念时,需要注意以下几个主要问题:

(1) 计算机系统关心的是信息用什么样的数据编码体制表示。例如,如何用ASCII码表示字母、数字与符号;如何用双字节去表示汉字;如何表示图形、图像与语音。对于数据通信技术来说,它要研究的是如何将表示各类信息的二进制比特序列通过传输介质在不同计算机之间传输的问题。

(2) 物理层需要根据使用的传输介质与传输设备确定表示数据的二进制比特序列所采用的电信号编码方式。

(3) 在数据通信中,电信号有两种类型:模拟信号与数字信号。

(4) 电平幅度连续变化的电信号称为模拟信号。语音信号是典型的模拟信号。在传统的电话线路上传输的信号是语音的模拟信号。

(5) 计算机产生的电信号是用两种不同的电平表示0、1比特序列的电压脉冲信号,这种电信号称为数字信号。

需要注意的是,模拟信号在采用如移频键控FSK、振幅键控ASK与移相键控PSK等方法调制之后,可以用于传输二进制的数字信号。

因此,D的描述是不正确的。

答案:D。

2-2-3 分析:

(1) 同步是数字通信中必须解决的一个重要问题。同步是要求通信双方在时间基准上保持一致的过程。如果在数据通信中收发双方同步不良,轻者会造成通信质量下降,严重时

甚至造成系统不能工作。数据通信的同步包括以下两种类型：位同步、字符同步。

（2）位同步。

实现位同步的方法主要有以下两种：外同步法与内同步法。

外同步法是在发送端发送一路数据信号的同时，另外发送一路同步时钟信号。接收端根据接收到的同步时钟信号来校正时间基准与时钟频率，实现收发双方的位同步。

内同步法则是从自含时钟编码的发送信号中提取同步时钟的方法。曼彻斯特编码与差分曼彻斯特编码都是自含时钟编码方法。

（3）字符同步。

字符同步的方法主要分为同步传输、异步传输。

同步传输将字符组织成组，以组为单位连续传送。每组字符之前加上一个或多个用于同步控制的同步字符 SYN，每个数据字符内不加附加位。

异步传输的特点是：每个字符作为一个独立的整体进行发送，字符之间的时间间隔可以是任意的。为了实现字符同步，每个字符的第一位前加 1 位起始位（逻辑 1），字符的最后一位后加 1 或 2 位终止位（逻辑 0）。

同步通信比异步通信的传输效率要高，因此同步通信更适用于高速数据传输。

因此，D 的描述是不正确的。

答案：D。

2-2-4 分析：设计这道习题的目的是帮助读者掌握双绞线的特点。

（1）双绞线是局域网中最常用的传输介质。双绞线可以由 1 对、2 对或 4 对相互绝缘的铜导线组成。一对导线可以作为一条通信线路。

（2）局域网中所使用的双绞线分为两类：屏蔽双绞线 STP 与非屏蔽双绞线 UTP。屏蔽双绞线由外部保护层、屏蔽层与多对双绞线组成；非屏蔽双绞线由外部保护层与多对双绞线组成。在典型的 Ethernet 网中，常用的非屏蔽双绞线 UTP 有 3 类线与 5 类线。随着千兆以太网 GE 等高速局域网的出现，各种高带宽的双绞线不断推出，如超 5 类线、6 类线与 7 类线。

（3）每对导线相互绞合的目的是为了使通信线路之间的电磁干扰达到最小，而不可能使线路向外部辐射的电磁达到最小。

因此，C 的描述是不正确的。

答案：C。

2-2-5 分析：设计该例题的目的是帮助读者了解光纤结构的特点，需要注意以下几点：

（1）光纤是传输介质中性能最好、应用前途最广泛的一种。光纤的纤芯是一种直径为 8～100μm 的柔软的、能传导光波的玻璃或塑料纤维，其中用超高纯度石英玻璃纤维制作的纤芯传输损耗最低。多条光纤组成一束构成一条光缆。

（2）在折射率较高的纤芯用折射率较低的包层包裹起来，外部再包裹涂覆层，这样就构成了一条光纤。

（3）由于光纤的折射系数高于外部包层的折射系数，因此可以形成光波在光纤与包层的界面上的全反射。光纤通过内部的全反射来传输一束经过编码的光信号。

因此，D 的描述是不正确的。

答案：D。

2-2-6 分析：了解光纤传输的特点，需要注意以下几点：

(1) 由于光纤的传输速率高、误码率低、安全性好，因此它成为了计算机网络中最有发展前景的传输介质。同时，由于光纤通信技术的发展，光纤组网成本的降低，光纤已经从主要用于连接广域网核心路由器，逐渐发展到城域网、局域网，目前正在向光纤直接接入办公室、接入家庭的方向发展。

(2) 由于光纤只能够单方向传输光载波信号，因此要实现计算机与交换机的双向传输就需要使用两根光纤。因此，B的描述是不正确的。

答案：B。

2-2-7 分析：了解有关光纤的物理层标准，需要注意以下几个问题。

(1) 影响光纤传输距离的因素主要有传输模式、光载波的频率、光纤的尺寸。

(2) 计算机产生的电信号需要在传输时变换成光载波信号在光纤上传播。由于光纤只能够单方向传输光载波信号，因此要实现计算机与交换机的双向传输就需要使用两根光纤。

(3) 在物理层协议中，用于从计算机向交换机传送信号的光纤称为上行光纤，用于从交换机向计算机传送信号的光纤称为下行光纤。上行光纤与下行光纤使用不同的光载波频率。

(4) 物理层协议规定的物理参数主要包括传输模式、上行光纤与下行光纤光载波的频率、光纤的尺寸、光接口，以及最大光纤传输距离。

例如，在传输速率为1Gbps的千兆以太网GE的物理层1000BASE-LX标准中，规定：传输介质采用单模光纤，光纤直径大于10μm，上行光纤与下行光纤的光载波的频率分别为1270nm与1355nm，光纤最大长度为5km。

UTP是Ethernet的10BASE-T的物理层非屏蔽双绞线的接口。因此，B的描述是错误的。

答案：B。

2-2-8 分析：设计该例题的目的是帮助读者了解光缆结构特点，需要注意以下几点：

(1) 光缆的缆芯包含多根光纤。

(2) 中心加强芯用来加强光缆的抗拉强度。中心加强芯是用高强度、低膨胀系数、抗腐蚀与有一定弹性的材料(如钢丝、钢绞线或钢管)制作。但是在强电磁干扰和雷区，则需要采用高强度的非金属材料。

(3) 护套是光缆的外部保护层，使得光缆在各种铺设条件下都能够具有很好的抗拉、抗压、抗弯曲能力。

(4) 按照光缆的使用环境，光缆可以分为架空光缆、直埋光缆、海底光缆、野战光缆等多种类型。目前，光缆在广域网、城域网与局域网，以及在电信传输网、广播电视传输网中都得到了广泛应用。

因此，D的描述是不正确的。

答案：D。

2-2-9 分析：了解ISM频段的特点，需要注意以下几点：

(1) 为了维护无线通信的有序性，防止不同通信系统之间的干扰，世界各国都要求使用者向政府管理部门申请特定的无线频段，获得批准后才可以使用。但是政府管理部门也专门划出了免予申请的频段，如工业、科学与医药专用的ISM频段。

(2) 用户在使用902～928MHz(915MHz频段)、2.4～2.485GHz(2.4GHz频段)、5.725～5.825GHz(5.8GHz频段)三个频段时,发送功率小于规定值(例如,在2.4GHz频段输出功率小于1W)时,可以不用申请。

(3) 计算机网络中,无线局域网Wi-Fi与其他无线通信系统中都在使用ISM频段。

因此,C的描述是不正确的。

答案:C。

2-2-10 分析:设计该例题的目的是帮助读者了解无线信号功率的计量单位,需要注意以下几点:

(1) 信号功率单位是瓦(W)或毫瓦(mW)。在无线局域网IEEE 802.11协议的讨论中,通常使用的是信号功率的相对值,即dBm。dBm是指信号功率相对于1mW的dB值。

(2) 计算公式为:$dBm = 10 \times \log_{10}(P_{mW})$,其中$P_{mW}$是信号以mW为单位的功率值。

(3) 1mW是一个参考点,0dBm表示1mW。如果测量值是+dBm,表示信号强度大于1mW;如果测量值是-dBm,表示信号强度小于1mW。

因此,C描述的计算公式是不正确的。

答案:C。

2-2-11 分析:了解无线主机之间通信的概念,需要注意以下几点:

(1) 无线通信中,描述无线信号的参数主要是频率与信号强度。

(2) 接收主机通过接收机接收无线信号有两个基本条件:一是发送信号频率要在接收机的频率范围之内;二是接收到的信号强度要大于接收机的接收灵敏度。

(3) 主机A接收机的频带为2.4500～2.4800GHz,主机B发送的信号频率为2.465GHz,主机B发送的信号频率在主机A的接收机频段之内。

(4) 接收机A的接收灵敏度都为-60dBm,而它实际接收到主机B无线信号的强度为-65dBm,低于主机A接收机的接收灵敏度。也就是说,接收信号太微弱了,主机A的接收机已经无法正确识别主机B发送的无线信号,因此主机A接收不到主机B发送无线信号的原因是信号太弱。因此,原因是D。

答案:D。

2-2-12 分析:了解微波段通信的特点,需要注意以下几点:

(1) 在电磁波谱中,频率在100MHz～10GHz的信号称为微波,它们对应的信号波长为3cm～3m。

(2) 微波信号传输的主要特点是:

- 微波信号绕射能力弱,微波信号只有在可视的情况下才能正常通信。
- 大气对微波信号的吸收与散射影响较大。由于微波信号的波长较短,因此利用机械尺寸较小的抛物面天线,就可以将微波信号能量集中在很小的波束中发送出去,这样可以用很小的发射功率来进行远距离通信。
- 微波信号的频率很高,可以获得较大的通信带宽,特别适用于卫星通信与城市建筑物之间的通信。

(3) 由于微波天线的高度方向性,因此在地面一般采用点对点方式通信。如果传输距离较远,可采用微波接力的方式作为城市之间的电话中继干线。在卫星通信中,微波通信也可以用于多点通信。

因此,A的描述是不正确的。

答案:A。

2-2-13 分析:了解蜂窝移动通信的特点,需要注意以下几点:

(1) 蜂窝移动通信属于电信行业移动通信的范畴。为了提高覆盖区域的系统容量与充分利用频率资源,人们提出了小区制的概念。由于区群的结构酷似蜂窝,因此小区制移动通信系统又称为蜂窝移动通信系统。

(2) 将一个大区制覆盖的区域划分成多个小区,在每个小区(cell)中设立一个基站,通过基站在用户的移动台之间建立通信。

(3) 小区覆盖的半径较小(一般为1~20km),可以用较小的发射功率实现双向通信。由若干个小区构成的覆盖区称为区群。区群中各小区的基站之间可以通过电缆、光缆或微波链路与移动交换中心连接。

(4) 1995年出现的第一代移动通信是模拟方式。1997年出现的第二代2G移动通信采用GSM、TDMA等数字制式,使得手机能够接入Internet。第三代3G移动通信能够在全球范围内更好地实现Internet的无缝漫游,使用手机来处理音乐、图像、视频,能够进行网页浏览,参加电话会议,开展电子商务活动,同时与第二代系统有良好的兼容性。3G的使用加速了手机通信网与Internet的业务融合,促进了移动Internet应用的发展。第四代4G移动通信技术正在推广过程,5G技术正在研究中。

因此,D的描述是不正确的。

答案:D。

2-2-14 分析:设计该例题的目的是帮助读者了解微波段通信的特点,需要注意以下几点:

由于卫星通信具有通信距离远、覆盖面积广、不受地理条件限制、费用与通信距离无关、可进行多址通信与移动通信的优点,因此卫星通信在近年来得到迅速发展,成为现代主要的通信手段之一。因此,D的描述是不正确的。

答案:D。

2.3 频带传输技术

2-3-1 分析:设计该例题的目的是加深读者对模拟数据编码方法的理解。在讨论模拟数据编码方法时,需要注意以下几个主要问题:

(1) 电话通信信道是典型的模拟通信信道,它是目前世界上覆盖面最广、应用最普遍的一类通信信道。传统的电话通信信道是为传输语音信号设计的,只适用于传输音频范围(300~3400Hz)的模拟信号,无法直接传输计算机的数字信号。为了利用模拟语音通信的电话交换网实现计算机的数字数据信号的传输,必须首先将数字信号转换成模拟信号。

(2) 将发送端数字数据信号变换成模拟数据信号的过程称为调制,将调制设备称为调制器;将接收端模拟数据信号还原成数字数据信号的过程称为解调,将解调设备称为解调器。具备调制与解调功能的设备称为调制解调器(modem)。

(3) 振幅键控方法是通过改变载波信号振幅来表示数字信号1、0。

(4) 移频键控方法是通过改变载波信号角频率来表示数字信号1、0。

(5) 移相键控方法是通过改变载波信号的相位值来表示数字信号1、0。

(6) 用相位的绝对值表示数字信号1、0,称为绝对调相;用相位的相对偏移值表示数字信号1、0,称为相对调相。

(7) 多相调制的方法可以将待发送的数字信号按两比特一组的方式组织,两位二进制比特可以有四种组合,称为四相调制;将发送的数据每三个比特组成一个三比特码元组,三位二进制数共有八种组合,称为八相调制。

因此,D关于八相调制的描述是错误的。

答案:D。

2-3-2 分析:设计该例题的目的是加深读者对数字数据编码方法的理解。在讨论数字数据编码方法时,需要注意以下几个主要问题:

(1) 基带传输是指基本不改变数字信号频带(即波形)直接传输数字信号的方法。

(2) 基带传输中数字信号编码方式主要有非归零码、曼彻斯特编码与差分曼彻斯特编码。

(3) NRZ码用高低电平分别表示逻辑0与1。NRZ码的缺点是无法判断一位的开始与结束,收发双方不能保持同步。为了保证收发双方的同步,必须在发送NRZ码的同时,用另一个信道同时传送同步信号。另外,如果信号中0与1的个数不相等时,存在直流分量,这在数据传输中是不希望存在的。

(4) 曼彻斯特编码的每个比特的中间有一次电平跳变,两次电平跳变的时间间隔可以是$T/2$或T,利用电平跳变可以产生收发双方的同步信号。第一个码元的起始$T/2$取数据的反码。因此,曼彻斯特编码信号称为“自含钟编码”信号,发送曼彻斯特编码信号时无须另外发送同步信号。

(5) 差分曼彻斯特编码是对曼彻斯特编码的改进。差分曼彻斯特编码与曼彻斯特编码不同之处在于:当数字为1时,在两个比特交接处不发生电平跳变;当数字为0时,交接处要发生电平跳变。

(6) 曼彻斯特编码与差分曼彻斯特编码的缺点是:需要的编码的时钟信号频率是发送频率的2倍。

需要注意的是,差分曼彻斯特编码与曼彻斯特编码的缺点相同,编码的时钟信号频率等于发送频率的2倍。因此,选项D是错误的。

答案:D。

2.4 基带传输技术

2-4-1 分析:

(1) 差分曼彻斯特编码规则。

① 每个比特的中间有一次电平跳变,两次电平跳变的时间间隔可以是$T/2$或T。

② 第一个码元的起始$T/2$取数据的反码。

③ 当数字为1时,在两个比特波形的交接处不发生电平跳变;当数字为0时,交接处要发生电平跳变。

(2) 具体到上图的信号波形。

第一个码元:前$T/2$为高电平,表示数据为0;

第二个码元:在比特波形的交接处没有发生电平跳变,表示第二位数据为1;

第三个码元：在比特波形的交接处没有发生电平跳变，表示第二位数据为1；

第四个码元：在比特波形的交接处发生电平跳变，表示第二位数据为0；

第五个码元：在比特波形的交接处没有发生电平跳变，表示第二位数据为1；

第六个码元：在比特波形的交接处没有发生电平跳变，表示第二位数据为1；

第七个码元：在比特波形的交接处没有发生电平跳变，表示第二位数据为1；

第八个码元：在比特波形的交接处发生电平跳变，表示第二位数据为0。

答案：差分曼彻斯特编码波形代表的数据是为01101110。

2-4-2 分析：设计该例题的目的是加深读者对PCM编码方法的理解。在讨论PCM编码方法时，需要注意以下几个主要问题：

(1) 脉冲编码调制PCM是模拟数据数字化的主要方法。PCM技术的典型应用是语音数字化。语音可以用模拟信号的形式通过电话线路传输，但是在网络中将语音与计算机产生的数字、文字、图形、图像同时传输，就必须首先将语音信号数字化。在发送端通过PCM编码器变换为数字化语音数据，通过通信信道传送到接收方，接收方再通过PCM解码器还原成模拟语音信号。

(2) PCM工作基本上包括采样、量化与编码三部分内容。

(3) 采样：模拟信号数字化的第一步是采样。模拟信号是电平连续变化的信号。采样是隔一定的时间间隔，将模拟信号的电平幅度值取出来作为样本，让其表示原信号。取样频率 f 应为 $f \leqslant 2B$ 或 $f=1/T \leqslant 2f_{max}$，式中，B 为通信信道带宽，T 为采样周期，f_{max} 为信道允许通过的信号最高频率。

(4) 量化：将取样样本幅度按量化级决定取值的过程。经过量化后的样本幅度为离散的量级值，已不是连续值。量化之前要规定将信号分为若干量化级，例如可以分为8级或16级，以及更多的量化级，这要看精度要求来定。同时要规定好每一级对应的幅度范围。然后将采样所得样本幅值与上述量化级幅值比较，取整定级。

(5) 编码：编码是用相应位数的二进制代码表示量化后的采样样本的量级。如果有 K 个量化级，则二进制的位数为 $\log_2 K$。例如量化级有16个，就需要4位编码。目前常用的语音数字化系统中多采用128个量级，需要7位编码。经过编码后，每个样本都用相应的编码脉冲表示。

(6) PCM用于数字化语音系统，将声音分为128个量化级，采用7位二进制编码表示。如果采样速率为8000样本/秒，数据传输速率应达到 7×8000b/s=56kbps。这个56kbps表示，传输该PCM系统所产生的数据需要占用的带宽至少为28kHz。

从以上分析中可以看出，D关于PCM数据速率的计算是错误的。

答案：D。

2-4-3 分析：设计该例题的目的是加深读者对信道速率概念的理解。在讨论信道速率概念时，需要注意以下几个主要问题：

(1) 奈奎斯特(Nyquist)准则与香农(Shanon)定律从定量的角度描述了“带宽”与“速率”的关系。

(2) 奈奎斯特准则指出：如果表示码元的窄脉冲信号以时间间隔为 $\pi/\omega(\omega=2\pi f)$ 通过理想通信信道，则前后码元之间不产生相互串扰。根据奈奎斯特准则，二进制数据信号的最大数据传输速率 R_{max} 与理想信道带宽 $B(B=f$，单位 Hz) 的关系可以写为 $R_{max}=2f$(bps)。

(3) 香农定理指出：在有随机热噪声的信道中传输数据信号时，传输速率 R_{max} 与信道带宽 B、信噪比 S/N 的关系为 $R_{max}=B\log_2(1+S/N)$。式中，R 单位为 bps，带宽 B 单位为 Hz。

(4) 在通信系统中，信噪比通常以分贝(dB)表示。如果信噪比 S/N 为 1000，根据信噪比计算公式 $S/N(\text{dB})=10\lg(S/N)$，则表示该信道的信噪比 S/N 为 30dB。

需要注意的是，在通信系统中，信噪比通常以分贝(dB)表示。如果 S/N 为 30dB，转换成十进制的比值应该是 1000。因此，D 的描述是错误的。

答案：D。

2-4-4 分析：设计该例题的目的是加深读者对香农定理的理解。在讨论香农定理时，需要注意以下几个主要问题：

(1) 香农定理指出：在有随机热噪声的信道上传输数据信号时，数据传输速率 R_{max} 与信道带宽 B，信号与噪声功率比 S/N 关系为 $R_{max}=B\log_2(1+S/N)$，式中，R_{max} 单位为 bps，带宽 B 单位为 Hz，信号与噪声功率比(简称信噪比)，通常用 dB(分贝)数表示。

(2) 已知 $S/N=30(\text{dB})$，那么信噪比根据公式 $S/N(\text{dB})=10\lg(S/N)$，可得 $S/N=1000$。

(3) 香农定律给出了一个有限带宽、有热噪声信道的最大数据传输速率的极限值。因为通信信道的最大传输速率与信道带宽之间存在着明确的关系，所以人们可以用“带宽”去取代“速率”。例如，人们常把网络的“高数据传输速率”用网络的“高带宽”去表述。因此“带宽”与“速率”在网络技术的讨论中几乎成了同义词。

计算：

(1) 已知 $S/N=30(\text{dB})$，那么根据公式 $S/N(\text{dB})=10\lg(S/N)$，可得 $S/N=1000$。

(2) 已知带宽 $B=3000\text{Hz}$。

(3) $R_{max}\approx 3000\times\log_2 1000\approx 30(\text{kbps})$。

答案：R_{max} 约为 30kbps。

2-4-5 分析：设计该例题的目的是加深读者对奈奎斯特准则与调制方式的理解。在讨论这个问题时，需要注意以下几个主要问题：

(1) 奈奎斯特准则：$R_{max}=2B(\text{bps})$

(2) QAM 调制方式表示：用四相位、每个相位用 4 种振幅表示数字信号，那么也就意味着可以用 16 种不同的物理状态来表示数据，即属于 16 相调制。

(3) 将线路带宽为 3kHz 与奈奎斯特准则联系起来，再用多相调制的波特率与比特率的关系就可以计算出线路的最大数据传输速率。

计算：

(1) 已知 $B=3\text{kHz}$，那么线路 $R_{max}\approx 3000\times 2=6(\text{kbps})$

(2) 已知 16 相调制，$S=R_{max}\log_2 k=6\times\log_2 16=6\times 4=24(\text{kbps})$

答案：线路的最大数据传输速率为 24kbps。

2.5 多路复用技术

2-5-1 分析：设计该例题的目的是加深读者对多路复用基本概念的理解。在讨论多路复用时，需要注意以下几个主要问题：

(1) 多路复用可以分为频分多路复用、波分多路复用、时分多路复用与码分多路复用。

(2) 时分多路复用是以信道传输时间为对象,通过为多个信道分配互不重叠的时间片的方法来达到多路复用的目的。

(3) 频分多路复用是以信道频率为对象,通过设置多个频率互不重叠的信道来达到同时传输多路信号的目的。

(4) 波分多路复用是在一根光纤上复用多路光载波信号。波分复用是光的频分多路复用。

(5) 码分多路复用也称为码分多址。码分多路复用是在同一频段的不同的信道采用经过特殊挑选的码型,使得在多个用户同时利用共享信道通信时相互之间不产生干扰。

从以上分析中可以看出,C对波分多路复用的描述是错误的。

答案:C。

2-5-2 分析:设计该例题的目的是加深读者对同步时分多路复用概念的理解。在讨论同步时分多路复用时,需要注意以下几个主要问题:

(1) 时分多路复用可以分为以下两类:同步时分多路复用与统计时分多路复用。

(2) 同步时分多路复用将时间片预先分配给各个信道,并且时间片固定不变,因此各个信道的发送与接收必须是同步的。同步时分多路复用采用将时间片固定分配给各个信道的方法,而不考虑这些信道是否有数据需要发送。

(3) 统计时分多路复用允许动态地分配时间片。

(4) 在动态时分复用中,时间片序号与信道号之间不存在固定的对应关系。

(5) 在时分多路复用的讨论中使用"帧"的术语。这里,"帧"是用来将物理层传送的比特流组织成一个个的数据单元,以便在接收端能够被正确地接收。因此,这里所说的"帧"与数据链路层"帧"的概念、作用不同,两者不能够混淆。

从分析中可以看出,D将时分多路复用中传输的"帧"与数据链路层的"帧"混淆了。

答案:D。

2-5-3 分析:

(1) 典型的频分多路复用系统结构如图2-1所示。

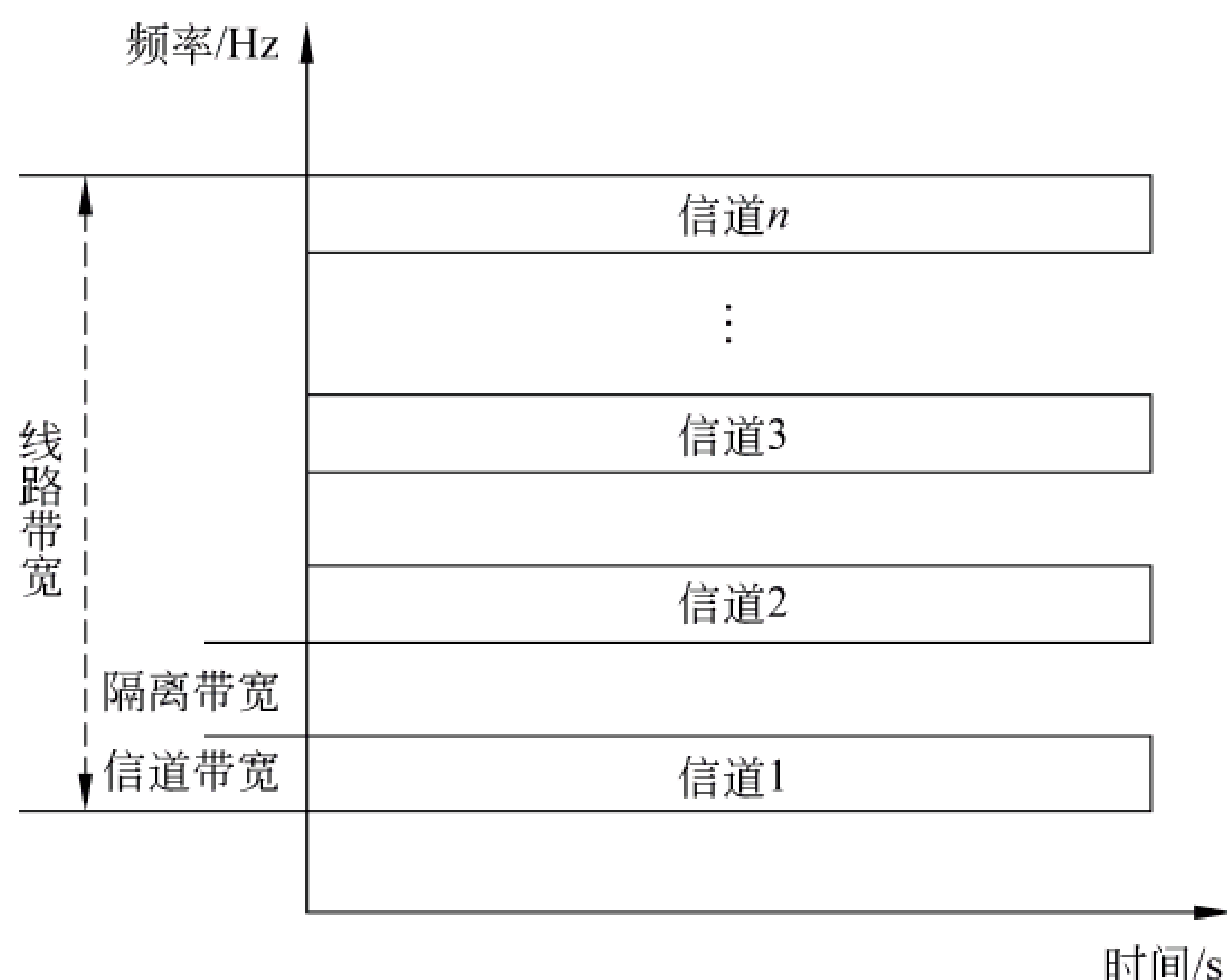


图2-1 频分多路复用系统结构示意图

(2) 设线路带宽为 B,信道带宽为 b,隔离带宽为 c。那么,信道数量

$$N \leqslant B/(b+c)$$

计算:

已知 $B=100\text{kHz}, b=3.2\text{kHz}, c=0.8\text{kHz}$,则

$$N=100/(3.2+0.8)=25$$

答案:在这条线路上用频分多路复用方法可以有 25 条信道。

2.6 同步光纤网 SONET 与同步数字体系 SDH

2-6-1 分析:设计该例题的目的是加深读者对基本速率标准的理解。在讨论基本速率标准时,需要注意以下几个主要问题:

(1) 在数据通信研究的初期曾经出现过多种速率标准,有的目前仍然在使用,主要有北美的 T1 载波速率、欧洲的 E1 载波速率以及 STM-1 速率等。

(2) T1 载波速率。

T1 载波速率是针对脉冲编码调制 PCM 的时分多路复用 TDM 设计的。T1 系统将 24 路音频信道复用在一条通信线路上。每路音频模拟信号的 PCM 编码器每秒取样 8000 次。24 路 PCM 信号轮流将 8b 插入到帧中。那么,每帧由 24×8=192b 组成,附加 1b 作为帧开始标志位,所以每帧共有 193b。发送一个帧需要的时间为 125μs。T1 载波的数据传输速率为

$$T1=((24\times8+1)/125)\times10^6=1.544(\text{Mbps})$$

(3) E1 载波速率。

由于历史的原因,与 T1 载波速率同时存在的还有不兼容的欧洲的 E1 载波速率。

E1 标准是 CCITT 标准。E1 标准将 30 路音频信道和 2 路控制信道复用在一条通信线路上。在一帧中为每个信道插入 1B(8b),这样一帧要传送的数据共 256b。传送一帧的时间为 125μs。E1 载波的数据传输速率为

$$E1=(32\times8/125)\times10^6=2.048(\text{Mbps})$$

(4) STM-1 速率。

STM-1 帧是一个块状结构,每行 270B,共 9 行,每秒发送 8000 帧。因此,STM-1 的传输速率应该为

$$\text{STM-1}=270\times8\times9\times8000=155.52\times10^6=155.52(\text{Mbps})$$

从以上讨论中可以看出,三种速率体系不兼容。其中,SDH 速率体系中,STS-1 速率是 51.84Mbps,三路复用后产生的 STS-1 速率等于 155.52(Mbps)。因此,D 是错误的。

答案:D。

2-6-2 分析:设计该例题的目的是加深读者对 SDH 速率体系基本概念的理解。在讨论 SDH 速率体系时,需要注意以下几个主要问题:

(1) SDH 定义了三种速率:SONET 的 STS、OC 速率标准、SDH 的 STM 标准。

(2) OC 定义的是光纤上传输的光信号速率。

(3) STS 定义的是数字电路接口的电信号传输速率。

(4) STM 标准是电话主干线路的数字信号速率标准。

(5) SONET 定义的电信号速率标准是以第 1 级同步传输信号 STS-1(51.84Mbps)为

基础,与其对应的是第1级光载波(Optical Carrier-1,OC-1)。

因此,C对于第1级电信号速率标准的描述是错误的。

答案:C。

2.7 接入技术

2-7-1 分析:设计该例题的目的是加深读者对接入技术基本概念的理解。在讨论接入技术时,需要注意以下几个主要问题:

(1) 接入技术关系到如何将成千上万的住宅、办公室、企业用户计算机接入Internet,关系用户能得到的网络服务的类型、应用水平、服务质量、资费等问题,同时也是城市网络基础设施建设中需要解决的一个重要问题。

(2) 用户接入可以分为家庭接入、校园接入、机关与企业接入。

(3) 接入技术可以分为有线接入与无线接入。

(4) 从实现技术的角度来看,宽带接入技术主要有数字用户线技术、光纤同轴电缆混合网技术、光纤接入技术、无线接入技术与局域网接入技术。

(5) 无线接入又可以分为无线局域网Wi-Fi接入、无线城域网WiMAX接入、蓝牙与ZigBee接入,以及无线移动通信网3G、4G接入等。

因此,D对于无线接入的描述是错误的。

答案:D。

2-7-2 分析:设计该例题的目的是加深读者对xDSL接入技术的理解。在讨论xDSL时,需要注意以下几个主要问题:

(1) 数字用户线(DSL)是利用一对电话线同时实现通话与上网的技术方案。

(2) 数字用户线包括非对称数字用户线(ADSL)、高速数据用户线(HDSL)、甚高速数据用户线(VDSL)等,因此人们通常是用前缀x来表示不同的数据用户线技术方案,统称为xDSL。

(3) 由于家庭用户主要是通过ISP从Internet下载文档,而向Internet发送信息的数据量不会很大。如果我们将从Internet下载文档的信道称为下行信道,将向Internet发送信息的信道称为上行信道,那么家庭用户需要的下行信道与上行信道的带宽是不对称的,因此ADSL技术很快就在家庭计算机联网中得到广泛应用。

(4) ADSL在电话线上同时提供电话与Internet接入服务,它提供的带宽具有非对称特性。

(5) 基于这样一种考虑,ADSL厂商与运营商提出了下行速率为1.5Mbps的ADSL标准G.Life,并于1999年获得ITU的批准,标准号是G.992.2。相对于预先设想的9Mbps速率,1.5Mbps小得多,因此,G.Life标准又称为"轻量级ADSL标准"。

(6) 近年来陆续公布了更高速率的第二代ADSL标准,如G.993与G.994的ADSL2标准、G.995的ADSL2+标准。其中,ADSL2+标准将频谱从1.1MHz扩大到2.2MHz,下行速率可以达到16Mbps,最大传输速率可以达到25Mbps,上行速率可以达到800kbps。

因此,D对ADSL2+标准传输速率的描述是错误的。

答案:D。

2-7-3 分析:设计该例题的目的是加深读者对HFC接入技术的理解。在讨论HFC接入技术时,需要注意以下几个主要问题:

(1) 20世纪60～70年代的有线电视网络技术只能提供单向的广播业务，那时的网络以简单共享同轴电缆的分支状或树形拓扑结构组建。随着交互式视频点播、数字电视技术的推广，用户点播与电视节目播放必须使用双向传输的信道，因此产业界对有线电视网络进行了大规模的双向传输改造。光纤同轴电缆混合网(HFC)就是在这样的背景下产生的。

(2) HFC技术的本质是用光纤取代有线电视网络中干线同轴电缆，光纤接到居民小区的光纤节点之后，小区内部接入用户家庭仍然使用同轴电缆，这样就形成光纤与同轴电缆混合使用的传输网络。传输网络形成以头端为中心的星形结构。

(3) 在光纤传输线路上采用波分复用的方法，形成上行和下行信道，在保证正常电视节目播放与交互式视频点播(VOD)服务同时，为家庭用户计算机接入Internet提供服务。

(4) 从头端向用户传输的信道称为下行信道，从用户向头端传输的信道称为上行信道。下行信道又需要进一步分为传输电视节目的下行信道与传输计算机数据信号的下行信道。

(5) 我国的有线电视网的覆盖面很广，通过对有线电视网络的双向传输改造，可以为很多的家庭宽带接入Internet提供一种经济、便捷的方法。因此，HFC已成为一种极具竞争力的宽带接入技术。

因此，C关于HFC网络拓扑结构的描述是错误的。

答案：C。

2-7-4 分析：设计该例题的目的是加深读者对光纤接入技术的理解。在讨论光纤接入技术时，需要注意以下几个主要问题：

(1) 光纤接入是指局端与用户端之间完全以光纤作为传输介质的接入方式。光纤接入可以分为有源光网络(AON)接入与无源光网络(PON)接入两类。同步光纤网SONET属于有源光网络，Internet接入主要采用无源光网络接入方式，在局端与用户端之间没有任何有源电子设备，通过无源的光器件构成光传输网络。

(2) 在讨论ADSL与HFC宽带接入方式时，我们已经了解到：用于远距离的传输介质已经都采用了光纤，只有临近用户家庭、办公室的地方仍然在使用电话线或同轴电缆。FTTx接入方式是将最后接入到用户端所用的电话线与同轴电缆全部用光纤取代。人们将多种光纤接入方式称为FTTx，这里的x表示不同的光纤接入地点。

因此，C关于家庭与办公室接入主要采用有源光网络接入方式的描述是错误的。

答案：C。

2-7-5 分析：设计该例题的目的是加深读者对不同光纤接入特点的理解。在讨论光纤接入技术的特点时，需要注意以下几个主要问题：

(1) 根据光纤深入到用户的程度，光纤接入可以进一步分为光纤到家(FTTH)、光纤到楼(FTTB)、光纤到路边(FTTC)、光纤到节点(FTTN)、光纤到办公室(FTTO)。

(2) 光纤到家是用一根光纤直接连接到家庭，省去了整个铜线设施(馈线、配线与引入线)，增加了用户的可用带宽，减少了网络系统维护工作量。

(3) 光纤到楼采用光纤到楼、高速局域网到户(即FTTB+LAN)，它是一种经济和实用的接入方式。使用FTTB不需要拨号，用户开机即可接入Internet，这种接入方式类似于专线接入。

(4) 光纤到路边是一种基于优化xDSL技术(即FTTC+xDSL)的宽带接入方式。这种接入方式适合于小区家庭已经普遍使用ADSL的情况。FTTC可以提高用户可用带宽，而

不需要改变ADSL的使用方法。FTTC一般采用小型的ADSL复用器DSLAM,部署在电话分线盒的位置,一般覆盖24～96个用户。

(5) 光纤到节点与FTTC很类似,它与FTTC的区别主要在于DSLAM部署的位置与覆盖的用户数。FTTN将光纤延伸到电缆交接盒,一般覆盖200～300个用户。FTTN比较适合用户比较分散的农场。

(6) 光纤到办公室FTTO与光纤到家FTTH很类似,只是光纤到办公室FTTO主要针对小型的企业用户。很显然,FTTO接入不但能够提供更大的带宽,简化了网络的安装与维护,而且能够快速引入各种新的业务,是最有发展前景的接入技术。

因此,C关于FTTO与FTTC区别的描述是错误的。

答案:C。

2-7-6 分析:设计该例题的目的是加深读者对无源光网络PON的特点的理解。在讨论无源光网络PON的特点时,需要注意以下几个主要问题:

(1) 由于光纤接入形成了从一个局端到多个用户端的传输链路,多个用户共享一条主干光纤的带宽,因此,无源光网络PON是一种点对多点的系统。光配线网ODN的典型拓扑结构为星形或树形。

(2) 光配线网ODN采用光波分复用,上、下行信道分别采用不同波长的光。

(3) 将无源光网络PON与广泛应用的Ethernet相结合形成的EPOS技术是目前发展最快、部署最多的PON技术。

(4) 为了适应更高速率的Ethernet技术,IEEE相继制定了802.3av 10Gbps EPON标准。802.3av标准在将下行速率提高到10Gbps的同时,与802.3ah标准保持很好的兼容性,使得10Gbps EPON与1Gbps EPON的光网络单元ONU共存于一个光配线网中,这样可以在持续提升接入带宽的同时,最大限度地保护了运营商的投资。

因此,B关于ODN拓扑结构的描述是错误的。

答案:B。

2-7-7 计算:

(1) A站的内积为 $S_A=(1+1+3+1-1-3-1-1)/8=0$,A站没有发送。

(2) B站的内积为 $S_B=(1-1-3-1-1-3+1-1)/8=-1$,B站发送了0。

答案:A站没有发送,B站发送了0。

2-7-8 分析:设计该例题的目的是加深读者对移动通信接入技术的理解。在讨论移动通信接入技术时,需要注意以下几个主要问题:

(1) 移动通信的主要概念包括接口、信道、移动台与基站。

(2) 无线通信中手机与基站通信的接口称为“空中接口”。所有通过空中接口与无线网络通信的设备通称为移动台。移动台可以分为车载移动台或手持移动台。手机就是目前最常用的便携式移动台。基站包括天线、无线收发信机、基站控制器(BSC)。

(3) 基站一端通过空中接口与手机通信,另一端接入到移动通信系统之中。手机与基站之间的无线信道包括手机向基站发送信号的上行信道,以及基站向手机发送信号的下行信道。上行信道与下行信道的频段是不同的。目前使用的4G的下行信道速率能够达到100Mbps,上行速率能够达到20Mbps。

(4) 每个地区的移动通信系统都是由地区移动交换中心的移动交换机(MSC)、归属位

置寄存器(HLR)、访问位置寄存器(VLR)与鉴权中心(AUC)服务器组成。

(5) 基站与手机之间是通过广播方式、点对多点方式连接,一个基站需要通过多个空中接口接收多个手机的信号。空中接口标准就是用于标识移动台,控制多个移动台对基站访问的通信协议。

(6) 3G/4G/5G 研究的是空中接口标准。2000 年 5 月,国际电信联盟(ITU)正式公布了 3G 标准——IMT—2000 标准,我国提交的时分同步码分多址(TD-SCDMA)正式成为国际标准,与欧洲宽带码分多址(WCDMA)、美国的码分多址(CDMA2000)标准一起成为 3G 主流的三大标准之一。

因此,D 关于 4G 特点的描述是错误的。

答案:D。

第三部分　综合练习——术语解析

从给出的 26 个定义中挑出 20 个,并将标识定义的字母填在对应术语前的空格位置。

(1) ________异步传输　　(2) ________多模光纤
(3) ________ 51.840Mbps　　(4) ________空中接口
(5) ________ ADSL　　(6) ________ FTTH
(7) ________ HFC　　(8) ________ ODN
(9) ________ FSK　　(10) ________ FTTC
(11) ________ PCM　　(12) ________基带传输
(13) ________ 0dBm　　(14) ________ CDMA
(15) ________光缆　　(16) ________比特率
(17) ________单模光纤　　(18) ________时分多路复用
(19) ________ 1.544Mbps　　(20) ________ ISM

A. 信号与光纤轴成多个可分辨角度的多路光载波传输模式。
B. 无线通信中手机与基站通信的接口。
C. 国际标准 ISO 646 信息交换编码。
D. 通过为多个信道分配互不重叠的时间片,达到同时传输多路信号的目的。
E. 为每个用户分配一种码型,多个用户同时使用一个信道而不互相干扰的方法。
F. SONET 中第一级光载波速率。
G. 允许动态分配时间片的方法。
H. 以字符为传输单元,字符之间的时间间隔可以是任意的。
I. T1 载波速率值。
J. 光纤到路边。
K. 无线信号功率为 1mW。
L. 信号与光纤轴成单个可分辨角度的单路光载波传输模式。
M. 由光纤缆芯、中心加强芯与保护套三部分构成的传输线路。
N. 由局端光线路终端 OLT、用户端光网络 ONU、无源光分路器 POS 组成的光网络。
O. 在模拟信道上传输数字信号的方法。

P. 通过改变载波信号角频率来表示数字信号1、0的方法。
Q. 将模拟的语音信号转化成数字语音信号的方法。
R. 为了提高数据传输速率,常用的多相调制的方法。
S. 光纤到家。
T. 每秒传送的构成代码二进制比特的数量,单位是bps。
U. 在数字信道上直接传送基带信号的方法。
V. 通过电话线路,并且上、下信道带宽不对称的接入方式。
W. 通过有线电视网络接入ISP的方式。
X. 无线通信中手机与基站的通信接口。
Y. 工业、科学与医药专用的免于申请的无线频段。
Z. 描述最大传输速率与信道带宽、信号噪声功率比之间关系的理论。

参考答案:

(1) H	(2) A	(3) F	(4) B	(5) V
(6) S	(7) W	(8) N	(9) P	(10) J
(11) Q	(12) U	(13) K	(14) E	(15) M
(16) T	(17) L	(18) D	(19) I	(20) Y

第 3 章 数据链路层

第一部分 同步练习

3.1 差错产生与差错控制方法

3-1-1 以下关于差错产生原因和差错类型的描述中,错误的是________。

A. 通信信道噪声是产生传输差错的主要原因

B. 通信信道的噪声分为热噪声和冲击噪声

C. 随机差错与突发差错构成了传输差错

D. 冲击噪声会产生随机差错

3-1-2 以下关于误码率概念的描述中,错误的是________。

A. 误码率是指二进制比特在数据传输系统中被传错的概率

B. 数值上近似等于被传错比特数与传输的二进制比特总数之比

C. 误码率是衡量数据传输系统异常工作状态下传输可靠性的参数

D. 被测量的传输二进制位数越大,才会越接近真正的误码率值

3-1-3 以下关于差错控制概念的描述中,错误的是________。

A. 自动检测出错误并进行纠正的方法称为差错控制方法

B. 为每个传输分组加上一定的冗余信息,接收端可以发现传输差错但不能纠正

C. 为每个传输分组加上足够多的冗余信息,以便接收端发现并自动纠正差错

D. 纠错码比检错码简单,实现起来容易

3-1-4 以下关于循环冗余编码特点的描述中,错误的是________。

A. 生成多项式 $G(x)$ 可以随机生成

B. CRC 校验码采用二进制的异或操作

C. CRC 校验码能检查出离散错与突发错

D. CRC 检错方法使用了双方预先约定的生成多项式 $G(x)$

3-1-5 如果发送数据比特序列为 11110011,生成多项式比特序列为 11001。请回答以下问题:

(1) 计算 CRC 校验序列。

(2) 给出发送方发送到接收方的比特序列。

3-1-6 如果发送的帧比特序列为110…1000001010,生成多项式$G(x)$的二进制比特序列长度为11010010,那么在发送的帧比特序列中包含的CRC校验比特序列为多少?

3-1-7 以下关于反馈重发纠错ARQ概念的描述中,错误的是________。

A. ARQ是指收发双方在发现帧传输错误时采用反馈重发来纠正错误的方法

B. 接收方通过校验码来判断数据传输中是否出错

C. 发送方在发送帧时保留发送数据字段的副本

D. 超过最大重发次数则停止发送,报告出错

3.2 数据链路层的基本概念

3-2-1 以下关于线路、链路、数据链路区别和联系的描述中,错误的是________。

A. 双绞线、同轴电缆、光纤属于通信线路(circuit)

B. 通信线路可以通过ASK方法分成多个信道(channel)

C. 发送器、接收器与通信信道共同构成一条链路(link)

D. 收发双方在数据链路设备之间构成一条数据链路(data link)

3-2-2 以下关于数据链路协议类型划分方法的描述中,错误的是________。

A. 数据链路层使用的链路有两类:点-点链路与广播链路

B. 点-点链路协议可以分为面向字符与面向比特型协议

C. 典型的局域网协议主要有IEEE 802.3协议、IEEE 802.11协议

D. 面向字符型协议主要有PPP协议

3-2-3 以下关于数据链路层功能的描述中,错误的是________。

A. 数据链路建立、维持和释放称为链路管理

B. 帧同步的作用主要是保证双方收发比特同步

C. "0比特插入/删除"的作用是保证帧传输的透明性

D. 差错控制使接收端能发现传输错误,并通过重传来纠正传输错误

3-2-4 以下关于数据链路层与网络层关系的描述中,错误的是________。

A. 数据链路层是OSI参考模型的第2层

B. 数据链路层向网络层屏蔽帧结构的差异性

C. 数据链路层使有差错的物理线路变为无差错的数据链路

D. 数据链路层必须实现链路管理、帧传输、流量控制、差错控制等功能

3-2-5 以下关于面向字符型协议帧结构特点的描述中,错误的是________。

A. 数据链路层协议可以分为两类:面向字符型与面向比特型

B. 面向字符型的协议通过定义一些标准字符来执行通信控制功能

C. BSC数据报用SOH字符表示正文的开始

D. 控制字符不能在用户数据字段中出现的现象称为用户数据不能"透明"传输

3.3 面向比特型数据链路层协议——HDLC协议

3-3-1 以下关于HDLC的帧结构的描述中,错误的是________。

A. HDLC帧由标志、地址、控制、信息、帧校验与标志等字段组成

B. 数据链路层的"帧"相当于OSI中的DL-PDU

C. HDLC 帧在信息字段中采用“0 比特插入/删除方法”

D. 网络层提交给的数据放在 HDLC 帧信息字段中

3-3-2 以下关于 HDLC 协议基本配置方式的描述中，错误的是________。

A. 数据链路配置分为非平衡配置与平衡配置

B. 非平衡配置可以用正常响应模式与异步响应模式

C. 在正常响应模式中，主站和从站可以随时相互传输数据帧

D. 平衡配置结构只有异步平衡模式

3-3-3 以下关于 HDLC 帧结构的描述中，错误的是________。

A. HDLC 帧结构包括固定部分和可选部分

B. HDLC 帧结构包括标志字段 F、地址字段 A 与控制字段 C

C. 标志字段 F 为 011111110 特定的比特序列

D. 为了解决数据传输的透明性问题，HDLC 协议采用“0 比特插入/删除方法”

3-3-4 发送的二进制比特序列为 0110 1111 1111 1100，如果封装在 HDLC 的数据字段中，经过“0 比特插入”处理之后的二进制序列应该是什么？

3-3-5 接收 HDLC 的数据字段二进制比特序列为 0001 1101 1111 0111 1101 10，经过“0 比特删除”处理之后的二进制序列应该是什么？

3.4 数据链路层滑动窗口协议及帧传输效率分析

3-4-1 以下关于 ARQ 协议类型和特点的描述中，错误的是________。

A. ARQ 实现方法有两种：单帧的停止等待方式和多帧的连续发送方式

B. 连续工作方式分为两种类型：拉回重发和选择重发纠错方式

C. 拉回重发纠错方式要求重发序号为 k 及以前的帧

D. 选择重发纠错方式只要求重传序号为 k 的帧

3-4-2 计算在无传输差错状态下执行 ARQ 停止-等待协议的效率。

条件：链路长度为 1000m，帧长度为 1000b。

计算：对应数据传输速率分别为 1kbps 与 10Mbps 的协议效率。

3-4-3 已知：传播延时为 20ms，节点发送速率为 100kbps。对于一个理想链路上采用的 ARQ 停止等待协议，如果效率要达到 0.6，那么帧长度最小为多少比特？

3-4-4 卫星通信系统采用停止等待 ARQ 协议。已知：一个卫星通信系统从地球到卫星的单向传播延时为 270s，数据帧长度为 1000b，数据发送速率为 500kbps。计算协议效率。

3-4-5 一个 IEEE 802.11b 无线局域网系统采用停止等待 ARQ 协议。已知：数据发送速率为 11Mbps；最大传输距离为 100m；数据帧长度为 1500B。计算协议效率。

3-4-6 以下关于反馈重发 ARQ 机制的描述中，错误的是________。

A. 发送方将数据校验字段一起发送到接收端

B. 接收方通过检错码检查数据帧是否出错，一旦出错，采用反馈重发方法纠正

C. 发送方在发送数据帧之后就可以不保留该帧的副本

D. 如果数据传输正确，接收方向发送方发送 ACK 确认信息

3-4-7 数据链路发送窗口 $W_s=4$，在发送 3 号帧、接收到 2 号帧的确认之后，发送方还能够

发送的帧数是________。

A. 1 B. 2 C. 3 D. 4

3-4-8 在以下滑动窗口概念的描述中,错误的是________。

A. 多帧、连续工作 ARQ 机制引入滑动窗口的概念

B. 连续工作 ARQ 可以分为拉回(GBN)与选择重发纠错(SR)两种方式

C. 发送窗口 W_t 表示在没有接收到确认的情况下,发送方最多可以连续发送的帧数

D. 帧序号长度为三位，ARQ 能够使用的最大窗口范围为 16

3-4-9 以下关于连续工作 ARQ 方式的描述中,错误的是________。

A. 停止等待方式的优点是协议简单,但是协议效率低

B. 连续工作 ARQ 方式分为两种类型：拉回方式和选择重发方式

C. 选择重发方式只发送出错的帧

D. 拉回方式虽然重发的帧可能多一些,但是它的效率高于选择重发方式

3-4-10 采取后退 N 帧 GBN 的拉回重发协议中,发送方已经发出编号为 0～5 的帧,当计时器超时,只收到接收方对 0、1、3、4 号帧的确认。那么发送方需要重发哪几个帧?

3-4-11 采取选择重传 SR 协议中,发送方发出编号为 0～5 的帧,只收到接收方对 1 号帧的确认,0、2 号帧依次超时。那么发送方需要重发哪个或几个帧?

3-4-12 采取选择重传 GBN 协议中,数据传输速率为 16kbps,单向传播延时为 270ms,数据帧长度范围为 128512B;接收方总是以等长的帧回复确认。为了使信道利用率达到最高,帧序号的比特位至少为多少?

3.5 PPP 协议

3-5-1 以下关于 PPP 协议特点的描述中,错误的是________。

A. PPP 协议也广泛用于路由器之间的专用线路

B. PPP 协议可以用于点-点连接,也可以用于点对多点连接

C. 网络控制协议(NCP)用于建立和配置不同的网络层协议

D. 链路控制协议(LCP)用于建立、配置、管理和测试数据链路连接

3-5-2 以下关于 PPP 信息帧格式的描述中,错误的是________。

A. 信息帧的数据字段的长度可变,它包含着要传送的数据

B. 信息帧头包括标志字段、地址字段、控制字段与协议字段

C. 地址字段长度值为接收节点的地址

D. 协议字段值为 0021H 表示网络层使用 IP 协议

3-5-3 接收端接收到的 PPP 信息字段的十六进制数为：7D 5E FE 27 7D 5D 7D 5D 65 7D 5E。试根据字节填充规则还原出发送的数据。

3-5-4 以下关于 PPP 链路控制帧的描述中,错误的是________。

A. PPP 帧的协议字段值为 8021H 表示链路控制帧

B. 数据链路选项包括协商异步链路中将什么字符当作转义字符

C. 数据链路选项包括协商不传输标志字节或地址字节,将协议字段缩短为 1 字节

D. 在同步链路中,转义采用的"0 比特插入/删除"方法由硬件自动完成

3-5-5 以下关于 PPP 网络控制帧的描述中,错误的是________。

A. 网络控制帧可以用来协商是否采用报头压缩 CSLIP 协议

B. 网络控制帧可以配置网络层，并获取一个临时 IP 地址

C. 结束访问时网络控制帧断开网络连接并释放 IP 地址

D. 释放 IP 地址后再使用网络控制帧断开网络链路连接

第二部分　同步练习答案与解析

3.1　差错产生与差错控制方法

3-1-1　分析：设计该例题的目的是加深读者对差错产生的原因和差错类型的理解。在讨论差错产生的原因和差错类型时，需要注意以下几个主要的问题：

(1) 发送数据通过通信信道后与接收数据不一致的现象称为传输差错。

(2) 检查是否出现差错以及如何纠正差错的方法称为差错控制方法。

(3) 通信信道噪声是产生传输差错的主要原因。

(4) 通信信道的噪声分为两类：热噪声和冲击噪声。

(5) 热噪声是一种随机的噪声，由热噪声引起的差错是随机差错。

(6) 冲击噪声是由外界电磁干扰引起的。冲击噪声引起的传输差错是一种突发差错。引起突发差错的位长称为突发长度。

(7) 通信过程中产生的传输差错是由随机差错与突发差错共同构成的。

从以上分析中可以看出，D 关于冲击噪声引起差错性质的描述是错误的。

答案：D。

3-1-2　分析：设计该例题的目的是加深读者对误码率概念的理解。在讨论误码率时，需要注意以下几个主要的问题：

(1) 误码率是指二进制比特在数据传输系统中被传错的概率，它在数值上近似等于：$P_e = N_e/N$。其中，N 为传输的二进制比特总数，N_e 为被传错的比特数。

(2) 误码率是衡量数据传输系统正常工作状态下传输可靠性的参数。数据在通信信道中传输时一定会由各种原因出现错误，出现传输错误是正常的和不可避免的，但是一定要控制在一个允许的范围内。

(3) 对于一个实际的数据传输系统，不能笼统地说误码率越低就越好，要根据实际的传输要求提出误码率要求。在数据传输速率确定后，要求传输系统的误码率越低，则传输系统的设备就会越复杂，相应造价也就越高。

(4) 对于实际数据传输系统，如果传输的不是二进制位，需要折合成二进制位来计算。

(5) 差错的出现具有随机性，在实际测量一个数据传输系统时，只有被测量的传输二进制位数越大，才会越接近真正的误码率值。

从以上分析中可以看出，噪声是通信信道所固有的，数据在通信信道传输过程中一定会因为各种原因出现错误，误码率是衡量数据传输系统正常工作状态下传输可靠性的参数，而不是异常状态，这一点经常引起误解。因此，C 的描述是错误的。

答案：C。

3-1-3　分析：设计该例题的目的是加深读者对检错码概念的理解。在讨论检错码概念时，需要注意以下几个主要的问题：

(1) 在计算机通信中,自动检测出错误并进行纠正的方法称为差错控制方法。

(2) 纠错码:为每个传输的分组加上足够多的冗余信息,以便接收方能发现并自动纠正传输差错。

(3) 检错码:为每个传输的分组加上一定的冗余信息,接收方可以根据这些冗余信息发现传输差错,但不能确定是哪一位或哪些位出错,并且自己不能够纠正传输差错。

(4) 检错码方法需要通过重传机制达到纠错目的。由于检错码工作原理简单,实现起来比较容易,编码与解码速度快,因此得到了广泛的应用。

从以上分析中可以看出,检错码方法通过重传机制达到纠错目的,工作原理简单,实现起来比较容易。纠错码实现相对困难。

因此,D的描述是错误的。

答案:D。

3-1-4 分析:设计该例题的目的是加深读者对循环冗余编码(CRC)特点的理解。在讨论CRC时,需要注意以下几个主要的问题:

(1) CRC具有检错能力强与实现容易的特点,是目前应用最广泛的检错码编码方法。

(2) CRC检错方法的工作原理是:将要发送的数据比特序列当作一个多项式 $f(x)$ 的系数,在发送端用收发双方预先约定的生成多项式 $G(x)$ 去除,求得一个余数多项式。将余数多项式加到数据多项式后发送到接收端。在接收端,用同样的生成多项式 $G(x)$ 去除接收数据多项式 $f'(x)$,得到计算余数多项式。如果计算余数多项式与接收余数多项式相同,表示传输无差错;否则,表示传输有差错,由发送方重发数据,直至正确为止。

(3) 生成多项式 $G(x)$ 的结构及检错效果是经过严格的数学分析与实验后确定,是由数据链路层协议规定的。

(4) 实际的CRC校验码是采用二进制模二算法的异或操作生成的。

(5) 在实际的网络应用中,CRC校验码的生成与校验过程可以用软件或硬件来实现。

(6) CRC校验码除了能够检查出离散错,还能够检查出突发错。

从以上分析中可以看出,CRC生成多项式 $G(x)$ 由协议来规定,$G(x)$ 的结构及检错效果是经过严格的数学分析与实验后确定的。目前,已有多种生成多项式列入国际标准,如:

CRC-12 $G(x)=x^{12}+x^{11}+x^3+x^2+x+1$

CRC-16 $G(x)=x^{16}+x^{15}+x^2+1$

CRC-CCITT $G(x)=x^{16}+x^{12}+x^5+1$

CRC-32 $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

生成多项式 $G(x)$ 不是随机生成的。

因此,A的描述是错误的。

答案:A。

3-1-5 分析:设计该例题的目的是为了加深读者对CRC校验原理和计算方法的理解。讨论CRC校验的实现方法需要注意以下几个问题:

(1) 发送方生成数据多项式 $f(x)x^k$,其中 k 为生成多项式的最高幂的值减1。本例中生成多项式的最高幂的值为5,$k=5-1=4$。那么 $f(x)x^4$ 首先将发送数据比特序列左移4位为11110011 $\underline{0000}$,这里的 $\underline{0000}$ 用来放入余数。

注意：由于发送数据比特序列左移的目的是放余数，余数最大为 4 位，因此左移的位数 k 应该是生成多项式的最高幂值减 1。本例中 $k=5-1=4$。

(2) 将 $f(x)x^k$ 除以生成多项式 $G(x)$，得 $f(x)x^k/G(x)=Q(x)+R(x)/G(x)$。其中，式中 $R(x)$为余数多项式。

(3) 将 $f(x)x^k+R(x)$作为整体，从发送方通过通信信道传送到接收方。

计算：

(1) 生成 CRC 校验码

```
                         10101110   ←Q(x)
G(x)→11001 √111100110000   ←f(x)·x^k
             11001
             -----
              11101
              11001
              -----
               10010
               11001
               -----
                10110
                11001
                -----
                 11110
                 11001
                 -----
                  1110  ←R(x)
```

CRC 校验码 $R(x)=1110$。

(2) 将余数比特序列加到乘积中得

```
1 1 1 1 0 0 1 1    1 1 1 0
```

发送数据比特序列 | CRC校验码比特序列

带CRC校验码的发送数据比特序列

发送带有校验码的比特序列是 111100111110。

答案：(1) CRC 校验码为 1110。

(2) 发送的比特序列是 111100111110。

3-1-6 分析：设计该例题的目的是为了加深读者对 CRC 校验计算方法的理解。讨论 CRC 校验的实现方法需要注意以下几个问题：

(1) 发送方生成数据多项式 $f(x)x^k$，其中 k 将发送数据比特序列左移 k 位用来放余数。$k=N-1$。N 为生成多项式 $G(x)$的二进制比特位数。

(2) 将 $f(x)x^k$ 除以生成多项式 $G(x)$，得 $f(x)x^k/G(x)=Q(x)+R(x)/G(x)$。其中，式中 $R(x)$为余数多项式。

(3) 将 $f(x)x^k+R(x)$作为整体，从发送方通过通信信道传送到接收方。

根据以上分析可以看出，可以根据 $G(x)$的二进制比特位数 N 得出 k 值；在发送的帧比特序列的后 k 位即是校验码。

计算：从已知条件可以看出：

(1) $N=8$，则 $k=8-1=7$；

(2) 发送的帧比特序列为 110…1000001010；

(3) 校验码应该为0001010。

答案：CRC校验比特序列为0001010。

3-1-7 分析：设计该例题的目的是加深读者对反馈重发纠错ARQ概念的理解。在讨论反馈重发纠错ARQ概念时,需要注意以下几个主要的问题：

(1) 实际的数据通信系统中采用检错码,必须制定基于检错码的差错控制的反馈重发纠错ARQ协议与机制。

(2) 反馈重发纠错ARQ是指：收发双方在发现帧传输错误时采用反馈重发来纠正错误的方法。

(3) 发送方将数据经过校验码编码器产生校验字段,并将校验字段与数据通过传输信道发送到接收方,同时在发送缓冲区中保留发送数据帧的副本。

(4) 接收方通过校验码译码器判断数据传输中是否出错。如果数据传输正确,那么接收方通过反馈信号控制器向发送方发送"传输正确(ACK)"信息。

(5) 接收方的反馈信号控制器收到ACK信息后,将不再保留发送数据的副本。如果数据传输不正确,那么接收方向发送方发送"传输错误(NAK)"信息。

(6) 发送方的反馈信号控制器收到NAK信息后,将根据保留数据的副本重新发送,直至在协议规定的最大重发次数中正确接收为止。如果超过协议规定的最大重发次数,接收方仍然不能正确接收,发送方停止该帧的发送,同时向高层协议报告错误信息。

从以上分析中可以看出,C关于发送方只发送数据字段的描述是错误的。

答案：C。

3.2 数据链路层的基本概念

3-2-1 分析：设计该例题的目的是加深读者对线路、信道、链路、数据链路区别的理解。线路、信道、链路、数据链路这几个术语虽然简单,但是很重要,并且容易混淆,分析它们之间的区别和联系,对于帮助读者理解数据通信原理是有益的。图3-1给出了上述几个术语的关系示意图。

在讨论线路、链路、数据链路区别时,需要注意以下几个主要的问题：

(1) 通信线路是指用于传输数据信号的传输介质,如双绞线、同轴电缆、光纤等。通信线路通常被简称为线路(circuit)。一条点对点的线路中间没有任何交换节点。通信线路通常被称作物理线路(physical circuit)。

(2) 一根通信线路可以通过多路复用方式分成多个通信信道,典型的方式是在同轴电缆中采用时分多路复用TDM、频分多路复用FDM、码分多路复用CDMA的方法,以及在光纤中使用波分多路复用WDM方式。每个信道可以传输一路信号。通信信道经常被简称为信道(channel)。

(3) 发送方的数据信号由发送器通过信道传送到接收方,接收器接收到数据信号。发送器、信道与接收器就构成了一条传输数据信号的链路(link)。

(4) 为了保证数据信号通过链路传输过程中的可靠性,在链路的两端均设置有执行数据链路层协议的设备,它可以用硬件方式实现,也可以用软件方式实现。发送方的数据链路层设备、发送器、信道、接收器与数据链路层设备就构成了一条数据链路(data link)。

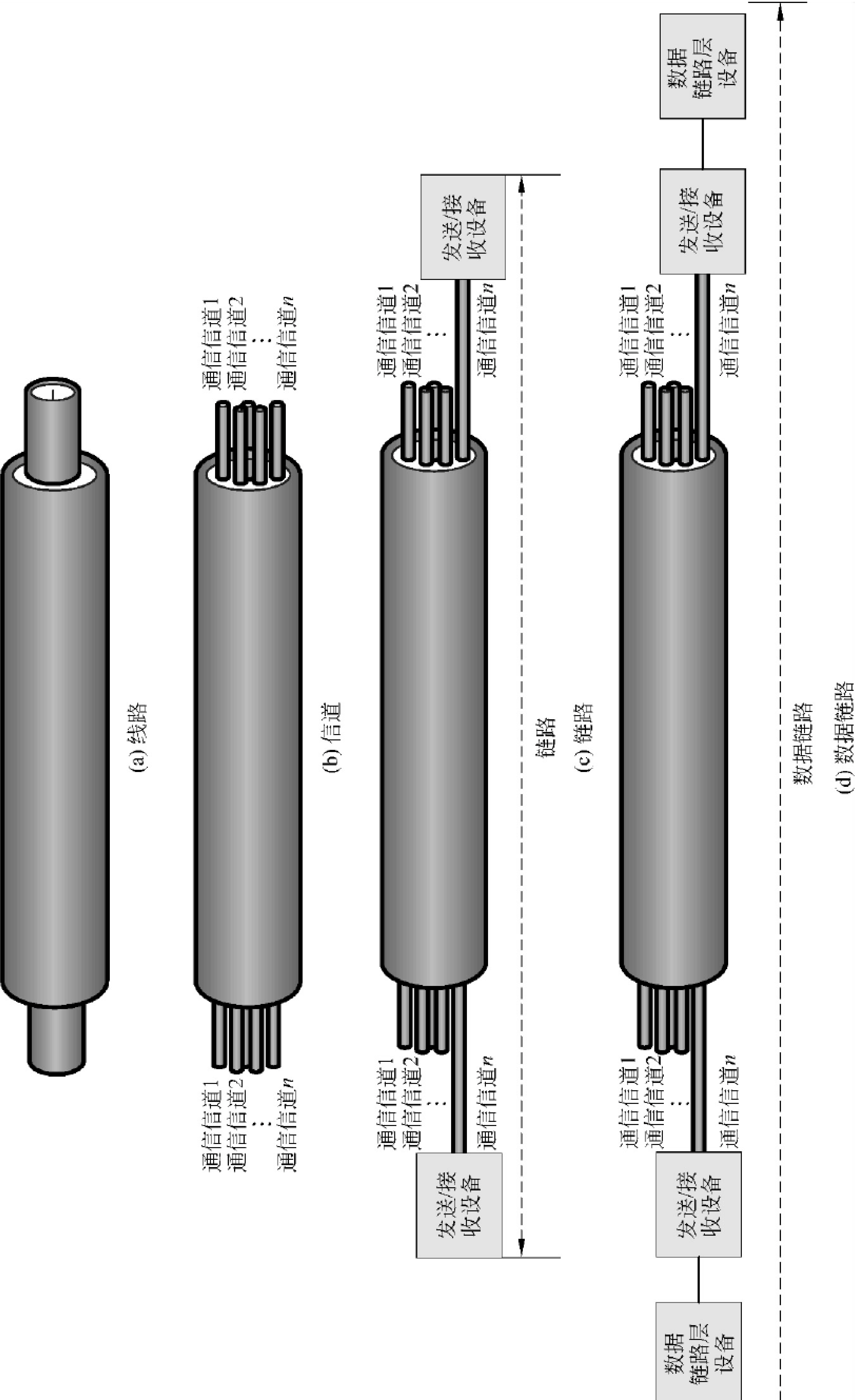


图 3-1　线路、链路与数据链路关系示意图

从以上分析中可以看出,B关于线路通过多路复用方法分成多个信道的描述是错误的。ASK是将数字数据信号变换成模拟数据信号在模拟信道上传输的方法,而不是多路复用方法。

答案:B。

3-2-2 分析:设计该例题的目的是加深读者对数据链路协议类型的理解。在讨论数据链路协议类型的划分时,需要注意以下几个主要问题:

(1) 数据链路层属于网络体系结构中的低层。数据链路层使用的链路有两类:点-点链路与广播链路。

(2) 点-点链路通过一条通信信道将两个节点直接连接起来,那么两个节点独占这一条通信信道,不存在多个节点竞争信道的问题。

(3) 广播链路中多个节点共享一条通信信道,必然存在多个节点竞争共享信道的问题。

(4) 正是因为节点在点-点链路与广播链路通信状态下工作机制不同,因此两类协议也就不同。

(5) 目前针对点-点链路的数据链路层协议可以分为两类:面向字符型协议与面向比特型协议。广泛应用的HDLC与PPP属于面向比特型的数据链路层协议。

(6) 广播链路主要针对局域网与无线网络。典型的局域网协议主要有IEEE 802.3的Ethernet协议、IEEE 802.11的WLAN协议与IEEE 802.16的无线城域网协议。广播链路的数据链路层协议主要是解决多个节点争用共享信道的控制和协调问题。

从以上分析中可以看出,D关于PPP协议类型的描述是错误的。

答案:D。

3-2-3 分析:设计该例题的目的是加深读者对数据链路层功能的理解。为了实现数据链路控制功能而制定的协议或规程称为数据链路层协议。数据链路层的功能主要有以下几点:

(1) 链路管理。

当两个节点要开始进行通信时,发送方必须确认接收方处在准备接收状态。双方必须先交换一些必要的信息,建立数据链路连接;同时,在传输数据时要维持数据链路;当通信完毕时,要释放数据链路。

(2) 帧同步。

数据在数据链路层以帧为单位传输。物理层的比特流按数据链路层协议的规定被封装在数据帧中传输。帧同步是指接收方应该能够从收到的比特流中正确地判断出一帧的开始位与结束位。

(3) 流量控制。

发送方的数据发送不能引起链路拥塞,并且接收方要能来得及接收。当链路出现拥塞或接收方来不及接收时,就必须控制发送方的数据发送速率。

(4) 差错控制。

计算机通信往往要求有极低的误码率,这样就必须采用差错控制技术。差错控制技术要使接收端能够发现传输错误,并在发送端的配合下纠正传输错误。

(5) 透明传输。

当传输的数据帧中出现控制字符时,就必须采取适当的措施,例如转义字符与“0比特

插入/删除”方法，使接收方不至于将数据误认为是控制信息。

（6）寻址。

在多点连接的情况下，要保证每一帧能传送到正确的目的节点。接收方也应该知道发送方是哪个节点，以及该帧是发送给哪个节点。

从以上分析中可以看出，B对帧同步作用的描述是错误的。

答案：B。

3-2-4 分析：设计该例题的目的是加深读者对数据链路层与网络层关系的理解。在讨论数据链路层时，需要注意以下几个主要问题：

（1）数据链路层介于物理层与网络层之间。

（2）设立数据链路层的主要目的是将原始的、有差错的物理线路变为对网络层无差错的数据链路。

（3）为了实现这个目的，数据链路层必须实现链路管理、帧传输、流量控制、差错控制等功能。

（4）数据链路层为网络层提供的服务主要表现在正确传输网络层的用户数据；为网络层屏蔽物理层采用的传输技术的差异性。

从以上分析中可以看出，数据链路层是向网络层屏蔽物理层采用的传输技术的差异性。因此，B的描述是错误的。

答案：B。

3-2-5 分析：设计该例题的目的是加深读者对面向字符型与面向比特型的协议特点的理解。在讨论面向字符型协议报文结构的特点时，需要注意以下几个主要问题：

（1）为了使原始的、有差错的物理线路成为无差错的数据链路，需要在物理层之上增加数据链路层。实现数据链路层的功能就需要制定相应的数据链路层协议。数据链路层协议可以分为两类：面向字符型与面向比特型。

（2）早期出现的数据链路层协议是面向字符型的协议。它的特点是利用已定义好的一种标准字编码（例如ASCII码、EBCDIC码）的一个子集来执行通信控制功能。

（3）在面向字符型的BSC协议中，使用ASCII码中的10个控制字符完成通信控制，并规定了数据与控制报文的格式，以及协议操作过程。

（4）BSC协议的数据报文格式是：

① 报头字段从SOH字符开始，报头字段是选项并由用户自行定义，例如存放地址、路径信息、发送日期等。

② 正文字段由STX字符开始，正文字段的长度未作规定，如果正文太长，则需要将正文分成几块传输，每块用ETB结束正文字段。

③ 当全部正文传输结束后，用ETX结束正文字段。BCC是校验字段。

（5）面向字符型协议有三个明显的缺点：

① 使用不同字符集的两台计算机很难利用面向字符型协议进行通信。

② 控制字符的编码（例如同步字符SYN编码为0010110）不能在用户数据字段中出现。这种现象称为用户数据不能“透明”传输。

③ 当正文字段中会出现控制字符时需要使用转义字符。

（6）为了克服这些缺点，在此基础上提出面向比特型协议，典型代表是ISO提出的高级

数据链路控制(HDLC)协议。

从以上分析中可以看出,BSC 数据报用 SOH 字符表示报头的开始,而不是正文的开始。

答案:C。

3.3 面向比特型数据链路层协议——HDLC 协议

3-3-1 分析:设计该例题的目的是加深读者对 HDLC 帧结构的理解。在讨论 HDLC 帧结构时,需要注意以下几个主要问题:

(1) 数据链路层的数据传输以帧为单位。这里的"帧"在 OSI 术语中是"数据链路协议数据单元(DL-PDU)"。

(2) HDLC 的帧结构具有固定的格式。网络层提交给数据链路层传输的数据放在 HDLC 帧的信息字段 I 中。数据链路层在信息字段的头尾各加上控制信息构成了一个完整的帧。

(3) HDLC 帧的组成为标志字段 F(8bit)、地址字段 A(8/16bit)、控制字段 C(8bit)、信息字段 I、帧校验字段 FCS(16bit)与标志字段 F(8bit)。

(4) HDLC 帧在地址字段 A、控制字段 C、信息字段 I、帧校验字段 FCS 采用 0 比特插入/删除方法,因此信息字段允许任意的二进制比特序列的组合。

(5) HDLC 帧校验字段对地址字段 A、控制字段 C、信息字段 I 进行校验。

从以上分析中可以看出,C 关于 HDLC 帧的 0 比特插入/删除范围的描述是错误的。

答案:C 是错误的。

3-3-2 分析:设计该例题的目的是加深读者对 HDLC 协议基本配置方式的理解。在讨论 HDLC 协议基本配置方式时,需要注意以下几个主要问题:

(1) 数据链路配置有两种:非平衡配置与平衡配置。

(2) 非平衡配置方式的特点:一组节点根据在通信过程中的地位分为主站与从站,由主站来控制数据链路的工作过程。主站发出命令;从站接受命令,发出响应,配合主站工作。

(3) 非平衡配置又可以分为两种类型,即点对点方式和多点方式。在多点方式的链路中,主站与每个从站之间都要分别建立数据链路。

(4) 非平衡配置可以有两种数据传送方式即,正常响应模式与异步响应模式。

• 正常响应模式(NRM)。

在正常响应模式中,主站可以随时向从站传输数据帧。从站只有在主站向它发送命令帧探询,从站响应后才可以向主站发送数据帧。

• 异步响应模式(ARM)。

在异步响应模式中,主站和从站可以随时相互传输数据帧。从站不需要等待主站发出探询就可以发送数据帧。但是,主站仍然负责数据链路的初始化、链路的建立、释放与差错恢复等功能。

(5) 平衡配置方式的特点是链路两端的两个站都是复合站。复合站同时具有主站与从站的功能,因此每个复合站都可以发出命令与响应。平衡配置结构只有一种工作模式,那就是异步平衡模式(ABM)。每个复合站都可以平等地发起数据传输,而不需要得到对方复合

站的许可。

HDLC 协议配置方式与数据传送方式是非常容易引起混淆的，设计该问题的目的是促使读者认真理解这些概念，这对了解协议设计方法是很有用的。比较具体内容之后会发现，人们会从字面的意义去认识"正常响应模式 NRM"与"异步响应模式 ARM"的内涵，C 正是初学者最容易出现的错误。

答案：C。

3-3-3 分析：设计该例题的目的是加深读者对 HDLC 帧结构的理解。在讨论 HDLC 帧结构时，需要注意以下几个主要问题：

(1) HDLC 的帧结构具有固定的格式。

(2) HDLC 帧结构包括：标志字段 F、地址字段 A 与控制字段 C。

(3) HDLC 规定在一个帧开头的第 1 个字节和结尾的最后 1 个字节的特殊标记。标志字段 F(flag)就是帧的开始与结束的标记。标志字段 F 为 01111110 特定的比特序列。为了解决数据传输的透明性问题，HDLC 协议规定采用"0 比特插入/删除方法"。

(4) 0 比特插入/删除方法规定：发送方在两个标志字段为 F 之间的比特序列中，如果检查出连续的 5 个 1，不管它后面的比特位是 0 或 1，都增加 1 个 0 比特位；在接收过程中，在两个标志字段 F 之间的比特序列中检查出连续的 5 个 1 之后就删除 1 个 0 比特位。

(5) 地址字段 A 长度是 8 位的整数倍。

(6) 控制字段 C 将 HDLC 帧划分为三类：信息帧(I)、监控帧(S)与无编号帧(U)。

从以上的分析中可以看出，HDLC 帧结构具有固定的格式。因此，A 的提法是错误的。

答案：A。

3-3-4 分析：HDLC 的"0 比特插入/删除"方法规定：发送端在两个标志字段 F 之间的比特序列中，如果检查出连续的 5 个 1，不管它后面的比特位是 0 或 1，都增加 1 个 0 比特位。

计算：

(1) 发送的二进制比特序列是 0110 1111 1111 1100。

(2) 插入后的二进制比特序列是 0110 1111 1011 1110 00。

答案：插入后的二进制比特序列是 0110 1111 1011 1110 00。

3-3-5 分析：设计这道习题的目的是帮助读者进一步理解 HDLC 的"0 比特删除"方法。

计算：

(1) 发送的二进制比特序列是 0001 1101 1111 0111 1101 10。

(2) 插入后的二进制比特序列是 0001 1101 1111 1111 1110。

答案：插入后的二进制比特序列是 0001 1101 1111 1111 111。

3.4 数据链路层滑动窗口协议及帧传输效率分析

3-4-1 分析：设计该例题的目的是加深读者对 ARQ 协议的类型和特点的理解。在讨论 ARQ 协议的类型和特点时，需要注意以下几个主要的问题：

(1) 在数据链路层的差错控制方法中，ARQ 实现方法有两种：单帧的停止等待方式和多帧的连续发送方式。连续工作方式又分为两种类型：拉回(GBN)重发纠错方式和选择重

发纠错方式。

(2) 在单帧的停止等待反馈重发纠错方式中,发送方每次发送一帧之后,需要等待确认帧返回之后再发送下一帧。停止等待方式的优点是协议简单,但是系统通信效率低。

(3) 在拉回(GBN)重发纠错方式中,发送方可以连续向接收方发送数据帧,接收方对接收到的数据帧进行校验,然后向发送方返回相应的应答帧。如果发送方发现序号为 k 的帧传输出错,则要求重新发送序号 k 及其已经正确发送的帧。

(4) 在选择重发纠错方式中,发送方可以连续向接收方发送数据帧,接收方对接收到的数据帧进行校验,然后向发送方返回相应的应答帧。如果发送方发现序号为 k 的帧传输出错,发送方只要求重传序号为 k 的帧。

从以上分析中可以看出,如果发送方在连续发送了编号为0~3帧后,从应答帧得知序号为1的帧传输错误,发送方将停止发送当前帧,并且重新发送序号为1、2、3帧。在拉回状态结束后,再继续发送4号帧。

因此,C关于拉回重发纠错方式要求重发序号为 k 及以前帧的描述是错误的。

答案:C。

3-4-2 分析:设计该问题的目的是加深读者对ARQ停止-等待协议的效率计算方法的理解。

(1) 在无传输差错状态下执行ARQ停止等待协议的效率计算公式为

$$U = 1/(1+2\alpha)$$

其中,α=传播延时/发送延时=t_p/t_f

(2) 已知:链路长度为1000m、帧长度为1000bit;

同时:电磁波传播速度约为 2×10^8m。

计算:

① 数据传输速率为1kbps:

传播延时 $t_p=1000/(2\times10^8)=5\times10^{-6}$(s)

发送延时 $t_f=1000/(1000)=1$(s)

$$\alpha = t_p/t_f = 5\times10^{-6}$$
$$U_1 = 1/(1+2\alpha)\approx 1$$

② 数据传输速率为10Mbps:

传播延时 $t_p=1000/(2\times10^8)=5\times10^{-6}$(s)

发送延时 $t_f=1000/(10\times10^6)=1\times10^{-4}$(s)

$$\alpha = t_p/t_f = 5\times10^{-5}/1\times10^{-4} = 0.05$$
$$U_2 = 1/(1+2\alpha)\approx 0.91$$

答案:数据传输速率为1kbps与10Mbps的协议效率分别为1与0.91。

3-4-3 分析:设计该问题的目的是加深读者对ARQ停止等待协议的效率计算方法的理解。

(1) 在无传输差错状态下执行ARQ停止等待协议的效率计算公式为

$$U = 1/(1+2\alpha) \quad 或 \quad U = t_f/(t_f+2t_p)$$

其中,t_p 为传播延时,t_f 为发送延时。

(2) 在上式中,已知 $U=0.6$,传播延时 $t_p=2\times10^{-3}$(s)。可以根据这两个数据计算出

发送延时 t_f，然后再根据发送速率计算出帧长度。

计算：

① 已知：$0.6=t_f/(t_f+2\times2\times10^{-3})$

得出：$t_f=6\times10^{-3}$(s)

② 已知：$t_f=L_f/S_t$

式中，L_f 为帧长度，S_t 为节点发送速率。已知 S_t 为 100kbps。

那么，$L_f=t_f\times S_t=6\times10^{-3}\times100\times10^3=600$(bit)

答案：帧长度最小为 600bit，效率可以达到 0.6。

3-4-4 分析：设计该例题的目的是结合数据链路层关于停止等待 ARQ 协议，计算在卫星通信系统传播延时较大情况之下的停止等待 ARQ 协议效率问题。

(1) 停止等待(ARQ)协议能够达到的帧传输效率为

$$U=1/(1+2\alpha)$$

其中，α＝传播延时/发送延时＝t_p/t_f。

(2) 本题已知传播延时 t_p，可以通过数据帧长度与数据发送速率计算出发送延时 t_f，因此可以计算出协议效率。

计算：

① $t_p=270$(s)

② $t_f=1000/(500\times10^3)=0.002$(s)

③ $\alpha=270/0.002=1.36\times10^4$

④ $U=1/(1+2\times1.36\times10^4)\approx3.7\times10^{-5}$

答案：采用停止等待 ARQ 协议的卫星通信系统的协议效率约为 3.7×10^{-5}。

3-4-5 分析：设计该例题的目的是结合数据链路层关于停止等待 ARQ 协议，计算在无线局域网通信系统传播延时较小情况下的停止等待 ARQ 协议效率问题。

计算的原理与上例相同。需要注意的是，无线局域网的电磁波在自由空间传播，传播速度为 3×10^8(m/s)。

计算：

① $t_p=100/3\times10^8\approx3.3\times10^{-7}$(s)

② $t_f=(1500\times8)/(11\times10^6)\approx1.09\times10^{-3}$(s)

③ $\alpha=3.3\times10^{-7}/1.09\times10^{-3}=3.03\times10^{-4}$

④ $U=1/(1+2\times3.03\times10^{-4})\approx1.0$

答案：在以上条件下的无线局域网通信系统停止等待 ARQ 协议效率约等于 1.0。

3-4-6 分析：设计该例题的目的是加深读者对 ARQ 实现机制的理解。

在讨论 ARQ 实现机制时，需要注意以下几个主要问题：

(1) 接收方通过检错码检查数据帧是否出错，一旦发现错误，通常采用反馈重发 ARQ 方法来纠正。

(2) 发送方将数据经过校验码编码器产生校验字段，并将校验字段与数据一起通过传输信道发送到接收端。

(3) 为了适应反馈重发的需要，发送方在存储器中保留发送数据的副本。

(4) 接收方通过校验码译码器判断数据传输中是否出错。如果数据传输正确，接收方

通过反馈信号控制器向发送方发送“传输正确(ACK)”信息。发送方的反馈信号控制器收到ACK信息后,将不再保留发送数据的副本。

(5) 如果数据传输不正确,接收方向发送端发送“传输错误(NAK)”信息。发送方的反馈信号控制器收到NAK信息后,将根据保留数据的副本重新进行发送,直至在协议规定的最大重发次数中正确接收为止。如果超过协议规定的最大重发次数,接收方仍然不能正确接收,那么发送方将向高层协议报告错误信息。

从以上分析中可以看出,C的描述是错误的。

答案:C。

3-4-7 分析:设计这道题目的目的是帮助读者深入理解发送窗口的概念。

(1) 在数据链路层差错控制的GBN方式与SR方式中,发送方不必等待接收方的确认ACK信息到来,就可以连续发送多个数据帧。但是从流量控制的角度,发送方可以连续发送帧的数量要受到接收方的限制。为了引入滑动窗口协议,人们定义了发送窗口与接收窗口。滑动窗口通过协调发送窗口 W_r 与接收窗口 W_s 值的方法来实现流量控制功能。

(2) 这里有一个问题需要注意:发送窗口长度为4还是发送窗口数量 $W_s=4$。很多教程在这个问题的表述上不够清晰。按照常规的不是方法,发送窗口长度为4,不是发送方可以连续发送 2^4 个帧,即可以发送编号为0、1、2……15共16个帧。从题意上看,应该理解为“发送窗口数量 $W_s=4$”,即发送窗口长度为2。发送方可以连续发送0、1、2、3号的4个帧。

(3) 题中表示“在发送3号帧、接收到2号帧的确认”,那么发送方还能够连续发送的帧是0、1、2,也就是还可以发送三个帧。

因此,C的数值是正确的。

答案:C。

3-4-8 分析:设计该例题的目的是加深读者对多帧滑动窗口与后退 N 帧协议(GBN)概念的理解。滑动窗口的概念在数据链路层与传输层的讨论中都会涉及。在讨论多帧滑动窗口与后退 N 帧协议(GBN)概念时,需要注意以下几个主要问题:

(1) 在多帧、连续工作的ARQ方式中,为了限制已经发出但没有被确认帧的数量,ARQ机制中引入了滑动窗口的概念。发送方与接收方分别设置了发送窗口与接收窗口。

(2) 发送窗口。

发送窗口 W_t 用于对发送方进行流量控制,它的大小表示:在没有接收到对方确认的情况下,发送方最多可以连续发送的帧数。例如,$W_t=4$ 表示在没有接收到对已发出帧的确认的情况下,发送方还可以继续发送4个帧。

发送窗口使用的规则是(假设发送窗口范围为2~5):

- 序号在发送窗口内的帧,即帧序号在2~5的帧,可以在它之前发出的序号为0、1等帧的确认没有到来的情况下连续发送。
- 每发送1帧之后,窗口不变,窗口大小减1。
- 如果连续发送了序号为5的帧,仍然未接收到之前发出的帧的确认,发送方停止发送,进入等待状态。
- 每接收到1个确认,发送窗口向前滑动1个帧的位置。
- 根据HDLC协议的规定,如果接收到序号为5的帧的确认,则表明序号为5及以前发送的帧都被正确接收。

（3）接收窗口。

接收窗口 W_R 的作用是控制接收数据帧的范围。

- 如果发送窗口范围为0～3，那么凡是帧序号在0～3的帧就接收；序号不在这个范围内的帧就丢弃。
- 如果正确接收到序号为0的帧，接收窗口就向前滑动一位，即接收窗口范围为1～4。

（4）在多帧、连续工作的反馈重发纠错方式中，ARQ可以分为两类：拉回重发（GBN）纠错方式与选择重发（SR）纠错方式。

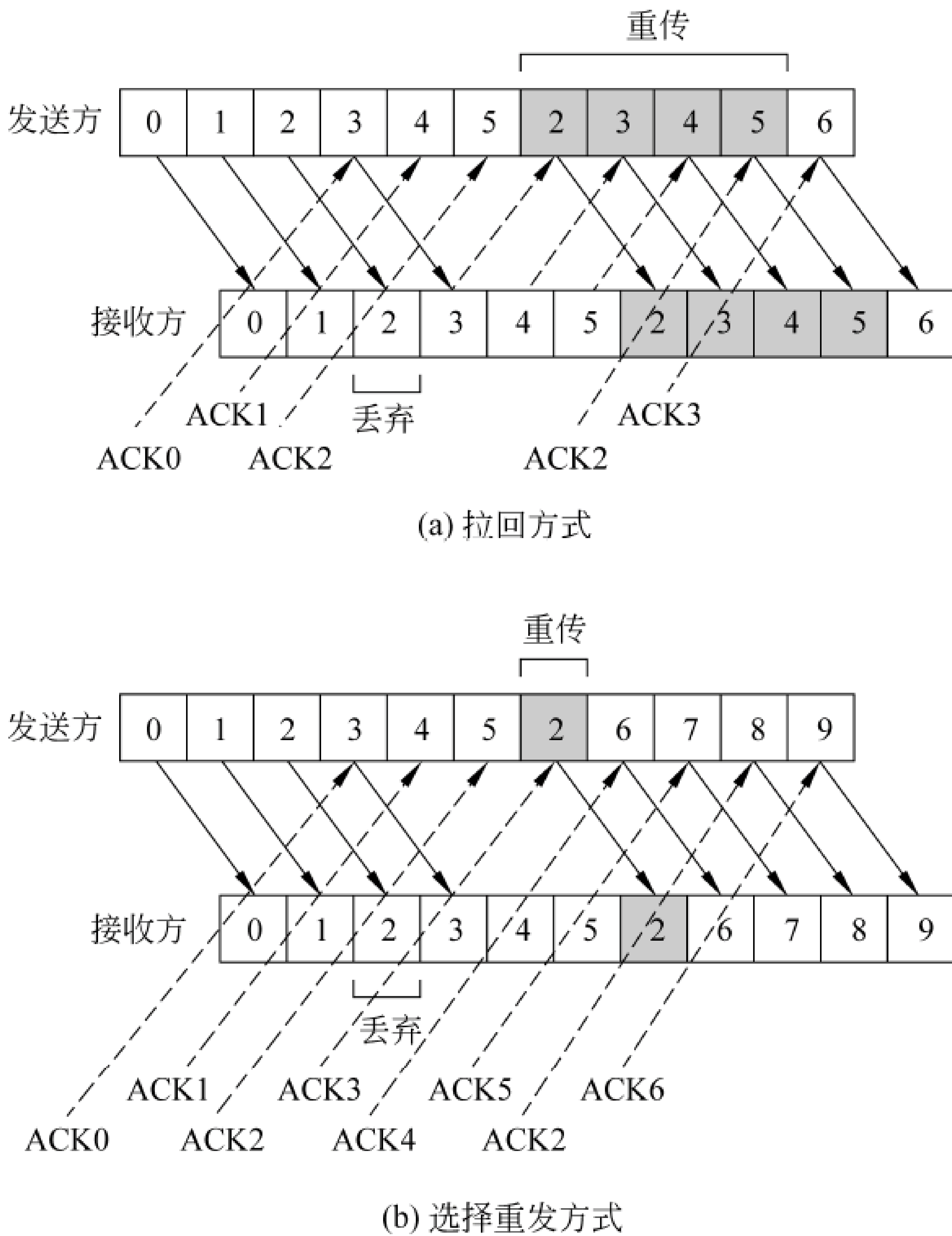
（5）滑动窗口值。

在HDLC帧结构中，发送帧序号 N(S)与接收帧序号 N(R)长度为3位，因此窗口最大长度为8。多帧连续发送的ARQ能够使用的最大窗口范围为 $2^3-1=7$。

从以上分析中可以看出，D对HDLC最大窗口范围的描述是错误的。

答案：D。

3-4-9 分析：设计该例题的目的是加深读者对连续工作ARQ选择重发方式的理解。图3-2给出了连续工作ARQ两种方式的工作原理示意图。



(a) 拉回方式

(b) 选择重发方式

图3-2 连续工作ARQ方式原理示意图

在讨论连续工作ARQ选择重发方式时，需要注意以下几个主要问题：

（1）ARQ实现方法有两种：停止等待方式和连续工作方式。停止等待方式的优点是协议简单，但是系统通信效率低。

(2) 连续工作 ARQ 方式又分为两种类型：拉回方式和选择重发方式。

(3) 在拉回方式中,发送方可以连续向接收方发送数据帧,接收方对接收到的数据帧进行校验,然后向发送方返回相应的应答帧。如果发送方在连续发送编号为 0~5 帧后,从应答帧得知 2 号帧传输错误,发送方将停止发送当前帧,并且重新发送 2、3、4、5 号帧。在拉回状态结束后,再继续发送 6 号帧。

(4) 选择重发方式与拉回方式的不同点在于：如果发送方在发送 5 号帧时,接收到 2 号帧传输出错的应答帧,则发送方在发送完 5 号帧后,只是重新发送出错的 2 号帧。在选择重发结束后,再继续发送 6 号帧。显然,选择重发方式的效率高于拉回方式。

从以上分析中可以看出,D 对两种工作方式协议效率的描述是错误的。

答案：D。

3-4-10 分析：设计这道练习题的目的是帮助读者理解后退 N 帧(GBR)拉回重发方式与选择重发(SR)方式的区别。

重发(SR)方式相对比较简单,哪个帧出错重传哪个帧。在后退 N 帧(GBR)拉回重发方式中,发送方可以连续向接收方发送编号为 0~5 的帧,接收方对接收到的数据帧进行校验,然后向发送方返回相应的应答帧。如果发送方只接收到编号为 0、1、3、4 的帧之后,从应答帧判断 2 号帧传输错误,发送方将拉回重新发送 2、3、4、5 号帧。在拉回状态结束后,再继续发送后续的帧。

答案：重发 2、3、4、5 号帧。

3-4-11 分析：设计这道练习题的目的是帮助读者理解选择重发(SR)方式的特点。

若采取选择重传 SR 协议,发送方发出编号为 0~5 的帧,已经收到 1 号帧的确认,0、2 号帧依次超时,那么发送方只需要重发 0、2 号帧。因为选择重发(SR)方式只根据是否在超时未接收到确认帧来决定是否需要重发。

答案：重发 0、2 号帧。

3-4-12 分析：设计这道习题的目的是帮助读者加深对拉回重发(GBN)方式工作过程的理解。

条件：

① 数据传输速率为 16kbps;

② 单向传播延时为 270ms;

③ 数据帧长度范围为 128~512B;

④ 接收方总是以等长的帧回复确认。

求：信道利用率达到最高时的帧序号的比特位长度。

GBN 工作过程如图 3-3 所示。

假设：帧长度为 L(512B>L>128B)

发送延时 $t_1 = L \times 8/16 \times 10^3$ (s)

传播延时 $t_2 = 270$ (ms)

(1) 发送一帧到收到确认的时间

$$T_0 = 2(t_1 + t_2) = 2(L \times 8/16 \times 10^3 + 270)$$

(2) 由于求解的是信道利用率达到最高时的帧序号的比特位长度,实际上是要求在发送一帧到收到确认的时间 T_0 内最多能够发送的帧数量 N_{max}。传播延时一定,为 270ms。

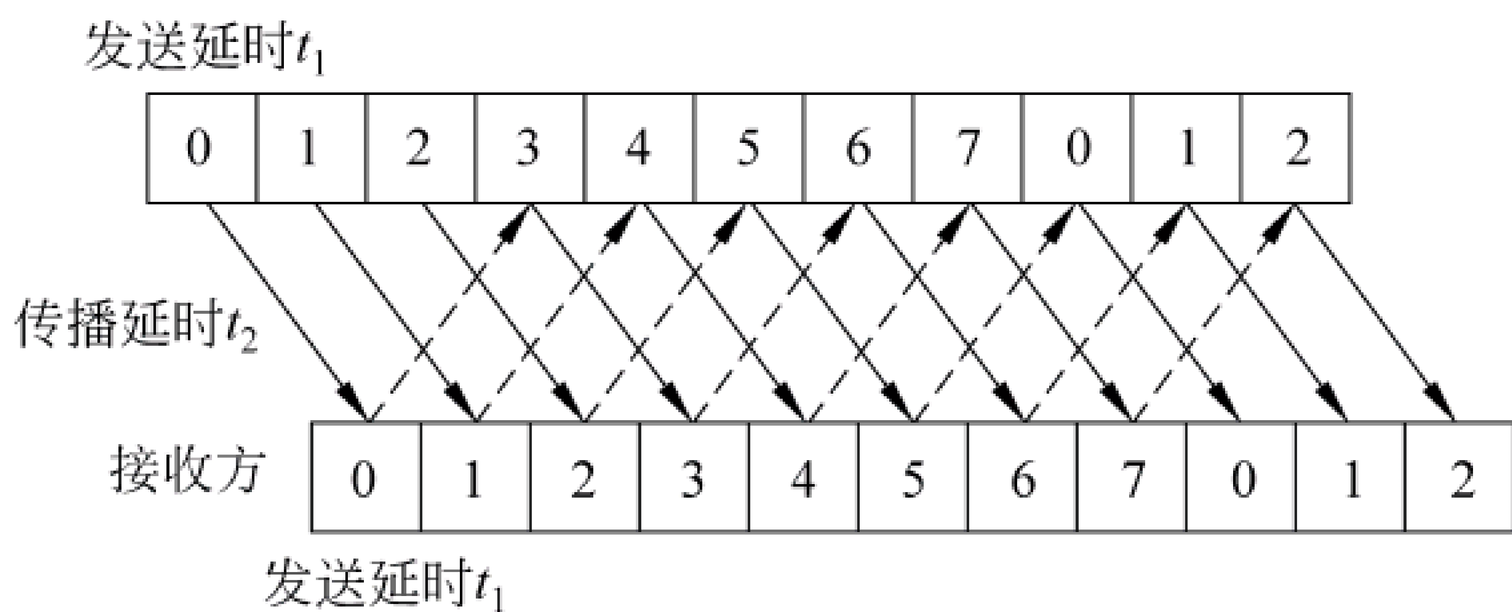


图 3-3　GBN 工作过程示意图

因此，L 必须取最小值 128B。

(3) $T_0=2(L\times 8/16\times 10^3+270)=668(\text{ms})$

在 T_0 时间内可以发送的帧数 $N_{max}=T_0/64=668/64\approx 10.43$(帧)

(4) 图 3-3 中使用的序号位数为 3，帧序号只能取 0～7；因此本题中帧序号位数取 4 时，可以满足要求。

答案：信道利用率达到最高时的帧序号的比特位长度为 4。

3.5　PPP 协议

3-5-1　分析：设计该例题的目的是加深读者对 PPP 协议特点的理解。在讨论 PPP 协议特点时，需要注意以下几个主要问题：

(1) 互联网数据链路层协议主要有两种：串行线路 IP 协议(SLIP)与点对点协议(PPP)。PPP 协议用于点对点的拨号电话线，是家庭或公司用户通过 ISP 方式连接到互联网的主要协议。同时 PPP 协议也广泛用于路由器之间的专用线路上。

(2) PPP 协议可以提供以下几种功能：

① 用于串行链路的基于 HDLC 数据帧封装机制。

② 链路控制协议(LCP)用于建立、配置、管理和测试数据链路连接。

③ 网络控制协议(NCP)用于建立和配置不同的网络层协议。

(3) PPP 协议的帧可以分为三种类型：PPP 信息帧、PPP 链路控制 LCP 帧和 PPP 网络控制 NCP 帧。

(4) PPP 协议不使用帧序号，不提供流量控制功能；只支持点-点连接，不支持点-多点连接；只支持全双工通信。

(5) 为了通过点-点的 PPP 链路进行通信，每个端点首先要发送 LCP 数据帧，以配置和测试 PPP 数据链路。当 PPP 链路建立起来后，每个端点发送 NCP 数据帧，以选择和配置网络层协议。当网络层协议配置好后，网络层的数据包可以通过 PPP 数据帧传输。

从以上的分析中可以看出，PPP 协议不使用帧序号，不提供流量控制功能；只支持点-点连接，不支持点-多点连接；只支持全双工通信。这是 PPP 协议有别于 HDLC 协议的重要特点。这些方面容易引起人们的忽视。因此，B 的描述是错误的。

答案：B。

3-5-2　分析：设计该例题的目的是加深读者对 PPP 帧格式的理解。在讨论 PPP 帧格式时，需要注意以下几个主要问题：

(1) PPP 帧格式由帧头、信息字段与帧尾 3 部分组成。PPP 信息帧的数据字段的长度

可变,它包含着要传送的数据,其开始部分可以是网络层的报头。

(2) PPP信息帧头包括以下4个部分:标志字段、地址字段、控制字段与协议字段。

(3) 标志字节长度为1字节,用于比特流的同步,采用HDLC表示办法,其值为7E(01111110),经常表示为0x7E。

(4) 地址字段长度为1字节,其值始终为FF(11111111),表示网中所有节点都能够接收该帧。

(5) 控制字段长度为1字节,取值为03(00000011)。

(6) 协议字段长度为2字节,它标识网络层协议数据域的类型。常用的网络层协议类型主要有:0021H表示TCP/IP;0023H表示OSI;0027H表示DEC;002BH表示Novell;003DH表示Multilink。

(7) PPP信息帧尾包括帧校验字段(FCS)字段与标志(flag)字段。

从以上的分析中可以看出,PPP协议用于点对点链路,因此地址字段长度值始终为FF(11111111)。因此,C的描述是错误的。

答案:C。

3-5-3 分析:为了解决使用异步通信时PPP协议的数据传输透明性问题,RFC1662定义了转义字符0x7D,并使用了字节填充。字节填充规则是:

(1) 在信息字段中出现的每个0x7E字节,要转换成双字节0x7D 0x5E。

(2) 在信息字段中出现的每个0x7D字节,要转换成双字节0x7D 0x5D。

(3) 在信息字段中出现ASCII中控制字符(即数值小于0x20)时,在该字符之前加一个0x7D字节,同时改变该字节。如传输结束ETX(0x03),转换后的双字节是0x7D 0x31。

计算:按照RFC1662定义的字节填充规则可以做出以下判断。

(1) 7D 5E还原后应该为7E。

(2) FE 27仍然为FE 27。

(3) 7D 5D还原后应该为7D。

(4) 7D 5D还原后应该为7D。

(5) 65仍然为65。

(6) 7D 5E还原后应该为7E。

因此,填充之前发送数据应为7E FE 27 7D 7D 65 7E。

答案:发送数据为7E FE 27 7D 7D 65 7E。

3-5-4 分析:设计该例题的目的是加深读者对PPP链路控制帧的理解。在讨论PPP链路控制帧时,需要注意以下几个主要问题:

(1) 在点对点链路中,主机接入需要经过三步:

① 呼叫ISP的路由器;

② 建立物理连接;

③ 发送链路控制帧,用来指定PPP协议的数据链路选项。

(2) PPP协议的数据链路选项主要包括:

① 协商异步链路中将什么字符当作转义字符。

② 协商是否可以不传输标志字节或地址字节,并且将协议字段从2字节缩短为1字节。

③ 如果在线路建立期间，收发双方不使用链路控制协商，那么固定的数据字段长度为1500B。

(3) PPP帧的协议字段值为C021H表示链路控制帧。在PPP链路传输的数据中出现与标志字节相同的字符时，也需要进行同样的转义处理。在同步链路中，转义采用的“0比特插入/删除”由硬件自动完成。

从以上分析中可以看出，PPP帧的协议字段值为C021H表示链路控制帧，协议字段值为8021H表示网络控制帧。因此，A的描述是错误的。

答案：A。

3-5-5 分析：设计该例题的目的是加深读者对PPP网络控制帧的理解。在讨论PPP网络控制帧时，需要注意以下几个主要问题：

(1) PPP帧的协议字段值为8021H表示网络控制帧。

(2) 网络控制帧可用来协商是否采用报头压缩CSLIP协议，也可用来动态协商确定链路每端的IP地址。

(3) 网络控制帧可以配置网络层，并获取一个临时IP地址。

(4) 当用户要结束这次访问时，网络控制帧断开网络连接并释放IP地址，然后使用链路控制帧断开数据链路连接。

从以上分析中可以看出，当用户要结束这次访问时，网络控制帧断开网络连接并释放IP地址，然后使用链路控制帧断开数据链路连接，而不是释放IP地址后再使用网络控制帧断开网络链路连接。因此，D的描述是错误的。

答案：D。

第三部分　综合练习——术语解析

从给出的26个定义中挑出20个，并将标识定义的字母填在对应术语前的空格位置。

(1) ________滑动窗口协议　　(2) ________面向字符型的协议

(3) ________标志字段　　(4) ________ LCP

(5) ________ U帧　　(6) ________突发长度

(7) ________ GBR　　(8) ________差错控制

(9) ________ SR　　(10) ________ link open

(11) ________检错码　　(12) ________配置请求帧

(13) ________透明传输　　(14) ________流量控制

(15) ________纠错码　　(16) ________误码率

(17) ________ NCP　　(18) ________ Link Establish

(19) ________ CHAP　　(20) ________捎带确认

A. 二进制比特在数据传输过程中被传错的概率。

B. 接收数据与发送数据不一致的现象。

C. 冲击噪声引起的差错比特位长度。

D. 能够自动纠正传输差错的编码。

E. 能够发现传输差错，但是不能自己纠正的编码。

F. 能够自动检测出传输错误并进行纠正的机制。
G. CRC 校验中发送方与接收方共同使用的一种多项式。
H. CRC 校验码计算时采用二进制算法。
I. 由传输介质与通信设备构成的线路。
J. 数据链路层保证帧中的二进制比特的组合不受任何限制的能力。
K. 利用标准字编码中的一个子集来执行通信控制功能的数据链路层协议。
L. HDLC 协议中由主站来控制从站通信的结构。
M. HDLC 规定用作帧开始与结束的标记字段。
N. HDLC 协议中起控制作用,可以随时发出,不影响带序号帧交换顺序的帧。
O. 数据链路层在差错控制与流量控制中采用的协议。
P. 发送方在连续发送过程中发现出错,并重新发送出错帧之后所有帧的纠错方法。
Q. 发送方在连续发送过程中发现出错,重新发送出错帧的纠错方法。
R. 发送序号与接收序号在差错控制中能够起到的作用。
S. 发送窗口与接收窗口能够实现的控制功能。
T. 广泛应用于 Internet 环境中路由器-路由器连接的数据链路层协议。
U. PPP 协议中用来建立、配置、管理和测试数据链路连接的协议。
V. PPP 协议中用来建立和配置网络层的协议。
W. 当用户计算机与路由器建立了物理层连接,PPP 进入的状态。
X. 当链路连接建立时,用户计算机首先向路由器发出的 LCP 帧。
Y. PPP 协议中需要通过三次握手来实现认证的协议。
Z. NCP 在网络层配置完成后链路进入的状态。

参考答案:

(1) O	(2) K	(3) M	(4) U	(5) N
(6) C	(7) P	(8) F	(9) Q	(10) Z
(11) E	(12) X	(13) J	(14) S	(15) D
(16) A	(17) V	(18) W	(19) Y	(20) R

第 4 章 介质访问控制子层

第一部分 同步练习

4.1 局域网技术的发展与演变

4-1-1 以下关于局域网拓扑结构的描述中，错误的是________。

A. 总线型局域网所有节点都通过网卡连接到一条作为公共传输介质的总线上

B. 当一个节点通过总线以“广播”方式发送数据时其他节点只能处于接收状态

C. 同一时刻出现两个或以上节点发送数据就会出现“冲突”

D. 传统的总线型 Ethernet 节点获得发送数据帧的时间是确定的

4-1-2 以下关于令牌总线工作原理的描述中，错误的是________。

A. 在令牌总线网中节点通过环接口连接成逻辑环形

B. 令牌是一种特殊结构的控制帧，用来控制节点对总线的访问权

C. 令牌总线网中每个节点两次获得令牌的最大时间间隔是确定的

D. 令牌协议在重负载情况下信道的利用率低

4-1-3 以下关于令牌环网的描述中，错误的是________。

A. 令牌环网的节点通过环接口连接成逻辑环形

B. IEEE 802.5 标准定义令牌环介质访问控制方法与相应的物理规范

C. 令牌帧中有一位标志令牌的忙/闲，当令牌空闲时节点可以使用该令牌发送数据帧

D. 令牌环网支持优先级服务

4-1-4 以下关于 IEEE 802 参考模型的描述中，错误的是________。

A. MAC 方法是指控制多个节点利用公共传输介质发送和接收数据的方法

B. 常用的 MAC 方法主要有 Token Ring、Token Bus 与 CSMA/CD

C. IEEE 802 参考模型将对应 OSI 参考模型中的数据链路层分为 LLC 子层与 MAC 子层

D. IEEE 802.2 标准定义了局域网各种物理层标准

4-1-5 Ethernet 的 CSMA/CD 算法提供的是________。

A. 无连接、不可靠服务

B. 连接、不可靠服务

C. 无连接、可靠服务

D. 连接、可靠服务

4-1-6 如果信号在传输介质上的传播速度为 2.3×10^8m/s,介质长度分别等于(1)网卡(10cm);(2)局域网(100m);(3)城域网(100km);(4)广域网(5000km)。计算:发送速率为1Mbps与10Gbps时的传播延时带宽积。

4-1-7 以下关于Ethernet技术发展趋势的描述中,错误的是________。

A. IEEE 802.3bs工作组研究速率达到100Gbps的下一代Ethernet网技术与标准

B. Ethernet网正在向云计算平台等后端计算机机房网络的方向发展

C. 工业Ethernet网正在广泛应用于工业自动化领域

D. IEEE 802.3az成为环保的EEE标准

4.2 Ethernet技术的研究与发展

4-2-1 以下关于CSMA/CD发送流程的描述中,错误的是________。

A. 先听后发　　B. 边听边发　　C. 冲突加强　　D. 延迟重发

4-2-2 以下关于CSMA/CD"冲突窗口"的描述中,错误的是________。

A. 冲突窗口长度为51.2μs

B. 冲突窗口的51.2μs可以发送64B数据

C. 64B是Ethernet的最小帧长度

D. 主机在发送一个帧前的64B没有发现冲突,仍然不能表明它已经成功获得总线发送权

4-2-3 在采用CSMA/CD算法的局域网中,如果总线长度为2000m,电磁波传播速度为 2×10^8m/s。主机A与B分别连接在总线的两端。

(1) 求:如果出现冲突,主机A与主机B能够检测到冲突的最短时间为多少?最长时间为多少?

(2) 如果没有出现冲突,主机A总是以最大帧长度(1518B)向主机B发送数据帧,主机B每接收到一个数据帧立即向主机A发送64B的确认帧;主机A在接收到确认帧之后才可以发送下一帧。

求:主机A每秒钟发送多少个数据帧?有效数据传输速率是多少?

4-2-4 如果在一个Ethernet网中,连接多台计算机的是一条同轴电缆。光速在同轴电缆中的传播速度为 2×10^8m/s。网卡的发送速率为1Gbps。如果最小帧长度减小600bit。那么连接在同轴电缆两端的计算机之间的距离是增加还是减小?变化量为多少米?

4-2-5 以下关于截止二进制指数后退延迟算法的描述中,错误的是________。

A. 算法可以表示为 $\tau=2^k\cdot R\cdot a$

B. a 是冲突窗口值

C. 以其MAC地址为初始值产生一个随机数 R

D. 最大可能延迟时间为1024个时间片

4-2-6 以下关于Ethernet V2.0与IEEE 802.3帧结构差异的描述中,错误的是________。

A. Ethernet V2.0规范定义的帧称作DIX帧

B. IEEE 802.3 标准定义的帧称为 802.3 帧

C. DIX 帧与 802.3 帧的帧校验字节不同

D. DIX 帧与 802.3 帧类型与长度字段不同

4-2-7 以下关于 IEEE 802.3 对“长度/协议字段”定义的描述中,错误的是________。

A. 定义 2B 的“长度/协议字段”

B. Ethernet 帧的最大长度小于 1500B

C. 用十六进制表示长度字段值一定小于 0x0600

D. IEEE 定义的协议字段值最小为 0x0800(IP 协议)

4-2-8 以下关于 Ethernet 帧 CRC 校验范围的描述中,错误的是________。

A. IP 伪报头

B. 目的地址

C. 源地址

D. 长度

4-2-9 以下关于 Ethernet“冲突加强”特点的描述中,错误的是________。

A. 检测出冲突第一步是发送“冲突加强信号”

B. 冲突加强信号长度规定为 64bit

C. 所有主机都能检测出冲突存在

D. 提高信道利用率

4-2-10 以下关于 Ethernet 帧接收过程的描述中,错误的是________。

A. Ethernet 主机只要不发送数据帧就应该处于接收状态

B. Ethernet 网卡完成一帧数据接收判断接收的帧长度

C. 帧长度小于规定的帧最小长度表明冲突发生

D. 向发送主机发生“传输出错通知”

4-2-11 以下包括在 Ethernet 网卡结构中的是________。

A. 网卡驱动程序

B. 链路控制器

C. 收发器

D. 解码器

4-2-12 以下关于 Ethernet 物理地址特点的描述中,错误的是________。

A. Ethernet 物理地址就是 MAC 地址

B. 网卡的 MAC 地址是全球唯一的

C. 网卡 MAC 地址由生产商分配

D. MAC 地址长度为 48bit

4-2-13 以下关于 802.3 X Type-Y Name 标准命名的描述中,错误的是________。

A. *X* 表示数据传输速率,单位为 Mbps

B. *Y* 表示网段的最大长度,单位为 1000m

C. Type 表示传输方式是基带还是频带

D. Name 表示局域网的名称

* **4-2-14** 根据 IEEE 802.3 标准的规定,Ethernet 的传输速率为 10Mbps,考虑帧间间隔,带

宽利用率为50%。请估算:

(1) 利用共享总线最多传输最大与最小帧长度的Ethernet帧各为多少?

(2) Ethernet的传输速率提高到为100Mbps时,每秒钟最多可传输最大与最小帧长度的Ethernet帧各为多少?

*4-2-15 假设条件:Ethernet总线长度为1000m,数据传输速率为10Mbps,信号在总线上的传播速度为2×10^8m/s。计算:能够使CSMA/CD算法成立的最短帧长度为多少?

分析:

(1) CSMA/CD算法成立的前提是在最短帧长度发送还未结束之前,总线上所有的节点都能够检查出是否发生冲突。因此,最短帧长度受到数据传播时间的约束。

(2) 已知总线长度L与信号传播速度V,就能够计算出信号从总线的一端传播到另一端所需要的传播时间。传播时间$\Delta t=L/V$。$2\Delta t$是CSMA/CD定义的冲突窗口值。

(3) 已知节点数据发送速率为S,那么$S\times2\Delta t$的值就是最短帧长度。

*4-2-16 Ethernet中只有两个节点,如果它们同时发送数据就会发生冲突,按二进制指数退避算法重传。重传的次数设为i,$i=1,2,3\cdots$。试计算第1次、第2次与第3次重传失败的概率,以及一个节点成功传输数据之前的平均重传次数。

*4-2-17 试估算Ethernet中节点每秒钟平均发送帧的数量。已知节点数为100,平均帧长度为1000b,传播延时为5μs/km。

条件:

(1) 总线长度为4km,发送速率为5Mbps。

(2) 总线长度为1km,发送速率为5Mbps。

(3) 总线长度为4km,发送速率为10Mbps。

*4-2-18 条件:在CSMA/CD算法中,总线长度为100m,信号在总线传输介质上的传播速度为2×10^8m/s,数据传输速率为1Gbps。

如果帧长度分别为512B、1500B与64000B,分别试估算并分析不同Ethernet帧长度的总线最大吞吐率。

4.3 交换式局域网与虚拟局域网技术

4-3-1 Ethernet交换机在决定转发策略时使用的是________。

A. 目的MAC地址

B. 源MAC地址

C. 目的IP地址

D. 源IP地址

4-3-2 以下关于交换式局域网的描述中,错误的是________。

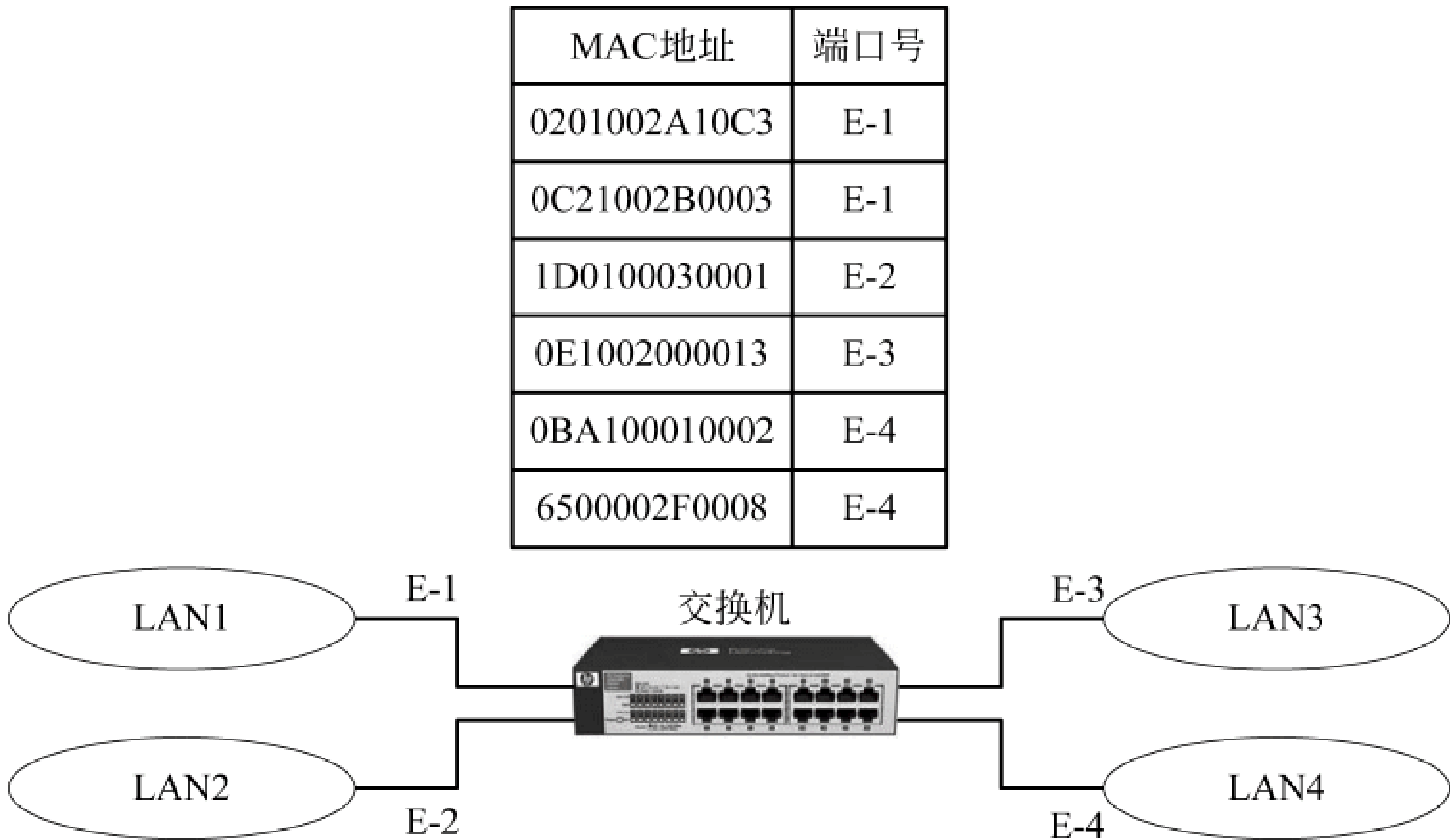
A. 交换机根据端口转发表找出对应的帧输出端口号

B. 地址学习是通过检查帧源地址与目的地址来建立转发表

C. 交换机交换方式主要分为直接、改进直接与存储转发交换方式

D. 改进直接交换方式的交换机需要接收帧前64B后才能决定是否转发该帧

4-3-3 用Ethernet交换机互联的网络结构如下图所示。



(1) 如果交换机从E-2端口接收到一个源地址为0010A13B5611、目的地址为08BA0011206B的帧。交换机应该完成的动作是什么?

(2) 如果交换机从E-2端口接收到一个源地址为0010A13B5611、目的地址为1D0100030001的帧。交换机应该完成的动作是什么?

4-3-4 以下关于VLAN概念的描述中,错误的是________。

A. VLAN是一种新型的局域网

B. 建立VLAN需要使用交换机

C. VLAN以软件方式来实现逻辑工作组的划分与管理

D. 逻辑工作组中的节点组成不受物理位置的限制

4-3-5 以下不能够用于VLAN划分的是________。

A. 传输层端口号　　B. 网络层协议

C. 网络层IP地址　　D. MAC层地址

4-3-6 以下关于IEEE 802.1Q协议的描述中,错误的是________。

A. IEEE 802.1Q用4B的VLAN标识来扩展Ethernet帧结构

B. 扩展帧结构包括2B的TPID与2B的TCI

C. 扩展的Ethernet帧TPID取值为0x6800

D. VID取值在1～4094

4.4 快速Ethernet的研究与发展

4-4-1 以下关于快速以太网的描述中,错误的是________。

A. 快速以太网标准是IEEE 802.3u

B. 速率自动协商功能在500ms内自动完成

C. IEEE 802.3u标准定义了MII将MAC层与网络层分隔开

D. 快速以太网保留传统的Ethernet的帧格式与最小、最大帧长度等特征

4-4-2 以下关于千兆以太网的描述中,错误的是________。

A. 千兆以太网已经不保留传统的 Ethernet 的帧格式与最小长度等特征
B. IEEE 802.3z 标准定义了千兆介质专用接口 GMII
C. 1000BASE-CX 使用两对屏蔽双绞线,双绞线最大长度为 25m
D. 1000BASE-ZX 使用单模光纤,光纤最大长度为 70km

4-4-3 以下关于 10GbE 特点的描述中,错误的是________。
A. 10GbE 标准是 IEEE 802.3ae
B. 10GbE 可以支持全双工与半双工方式
C. 10GbE 采用 OC-192/STM-64,速率是 9.95328Gbps
D. LAN PHY 标准根据使用的传输介质分为两类:光纤与双绞线

4-4-4 以下关于 40GbE 与 100GbE 的描述中,错误的是________。
A. 40GbE 技术将会大量应用于 IDC、高性能计算机、高性能服务器集群与云计算平台
B. 城域网与广域网核心交换网出现从 10GbE 向 40GbE、100GbE 的平滑过渡趋势
C. 100GbE 研究涉及 Ethernet 技术、密集波分复用 DWDM 传输技术等方面
D. 100GbE 采用的是 802.3ab 标准

4-4-5 以下关于光以太网与城域以太网的描述中,错误的是________。
A. 光以太网与城域以太网标志着 Ethernet 技术向城域网、广域网延伸
B. 光以太网的概念偏重于技术,城域以太网的概念更偏重于应用
C. 光以太网能够根据终端用户的实际应用需求分配带宽
D. 光以太网必须支持尽力而为的服务

4.5 Ethernet 组网设备与组网方法

4-5-1 以下关于集线器 hub 特征的描述中,错误的是________。
A. 节点通过非屏蔽双绞线与集线器连接
B. 集线器与连接的节点在物理结构上是总线形
C. 从节点到集线器的非屏蔽双绞线最大长度为 100m
D. 节点数超过单一集线器的端口数时可以采用多集线器级联的结构

4-5-2 计算以下三种情况之下每个节点可以得到的平均带宽。
(1) 10 个节点接到一台 10Mbps 的 Ethernet 集线器上。
(2) 10 个节点接到一台 100Mbps 的 Ethernet 集线器上。
(3) 10 个节点接到一台 10Mbps 的 Ethernet 交换机上。

4.6 局域网互联与网桥的基本工作原理

4-6-1 以下关于网桥概念的描述中,错误的是________。
A. 网桥能够在网络层实行网络互联
B. 网桥可以分隔两个网络之间的广播通信量
C. 网桥能够互联不同传输介质与不同传输速率的网络
D. 网桥以接收、存储、地址过滤与转发的方式实现互联网络之间的通信

4-6-2 以下关于网桥分类的描述中,错误的是________。

A. 路由表中记录了不同节点的 IP 地址与网桥转发端口关系

B. 网桥最重要的工作是构建和维护路由表

C. 透明网桥由各个网桥来决定路由选择

D. 源路选网桥由发送帧的源节点负责路由选择

4-6-3 以下关于透明网桥与生成树算法的描述中,错误的是________。

A. 透明网桥一般用在两个不同 MAC 层协议的网段之间的互联

B. 透明网桥的路由表要记录三个信息:站地址、端口与时间

C. 生成树算法最终创建一个逻辑上无环路的网络拓扑结构

D. 为了避免出现环状结构,透明网桥使用了生成树算法

4-6-4 以下关于源路由网桥的描述中,错误的是________。

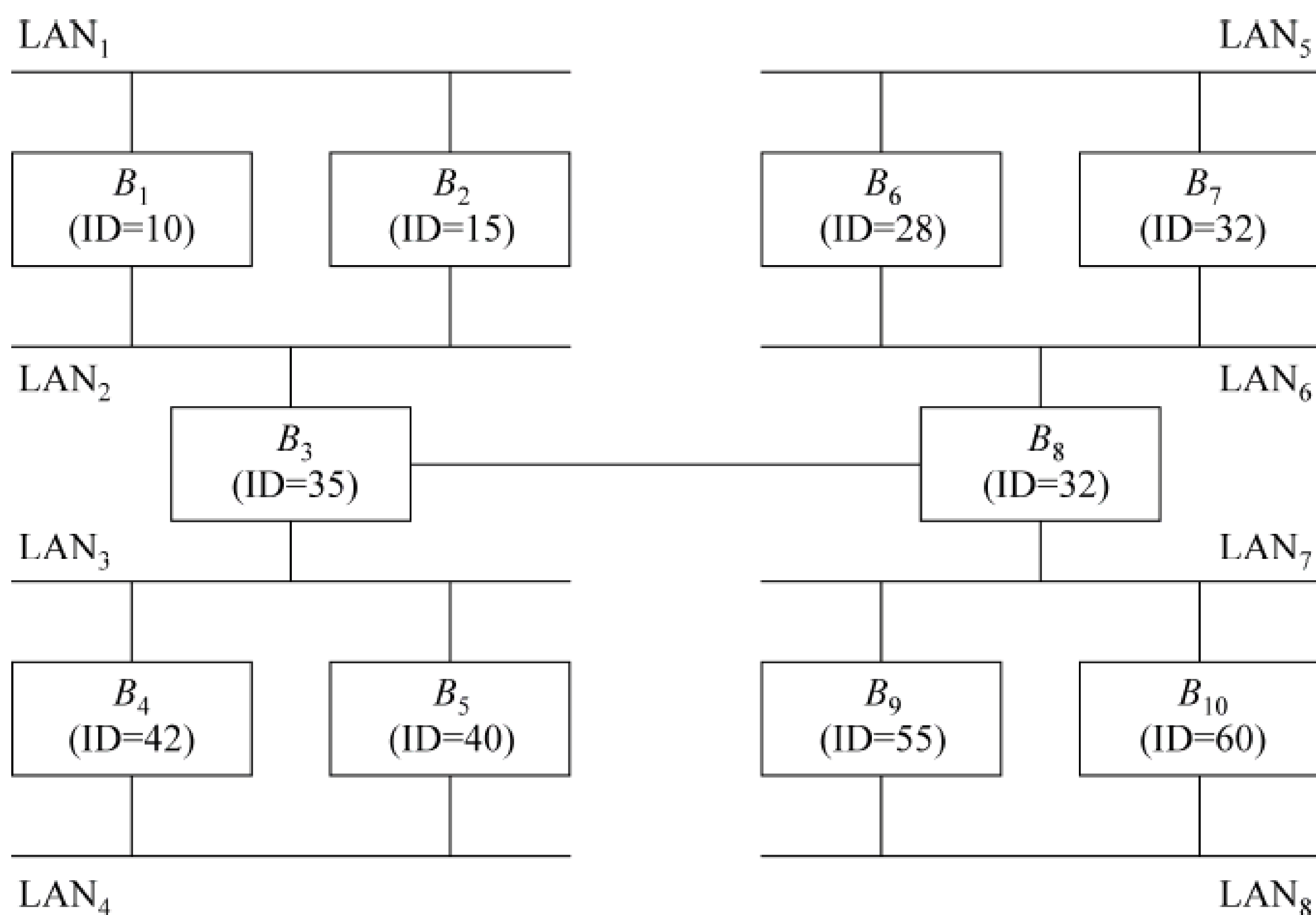
A. 为了发现适合的路由,源节点以广播方式向目的节点发送用于探测的发现帧

B. 如果有超过一条的路径,源节点将选择经过中间路由器最少的路径

C. 源路由网桥在发送帧头部写入路由信息

D. IEEE 802.5 制定源路由网桥标准

4-6-5 用 10 个网桥互联 8 个局域网的结构如下图所示。图中标记了各个网桥的 ID 值。假设 STP 协议在执行过程中只比较 ID 值的大小。按照生成树算法,画出互联结构图。



4.7 无线局域网

4-7-1 以下关于 IEEE 802.11n 标准特点的描述中,错误的是________。

A. 工作在 2.4GHz 频段

B. 可以动态地调整天线的方向

C. 速率最高可以达到 600Mbps

D. 接入点的覆盖范围可以达到几平方公里

4-7-2 以下关于千兆 Wi-Fi 标准 IEEE 802.11ad 特点的描述中,错误的是________。

A. 速率为 7Gbps

B. 工作频段在5GHz

C. 与IEEE 802.11a/b/g/n标准兼容

D. 更适应于家庭高速Internet接入应用

4-7-3 以下关于IEEE 802.11b协议规定的传输速率的描述中,错误的是________。

A. 1Mbps B. 2Mbps C. 8Mbps D. 11Mbps

4-7-4 以下关于IEEE 802.11的动态速率调整(DRS)技术特点的描述中,错误的是________。

A. IEEE 802.11协议规定了若干个传输速率

B. 无线网卡根据信号质量调整传输速率的一种反馈控制机制

C. 调整的依据是信号强度、信噪比与帧错误率

D. IEEE 802.11协议对DRS算法有具体的规定

4-7-5 以下关于IEEE 802.11物理层对2.4GHz频段信道划分方法的描述中,错误的是________。

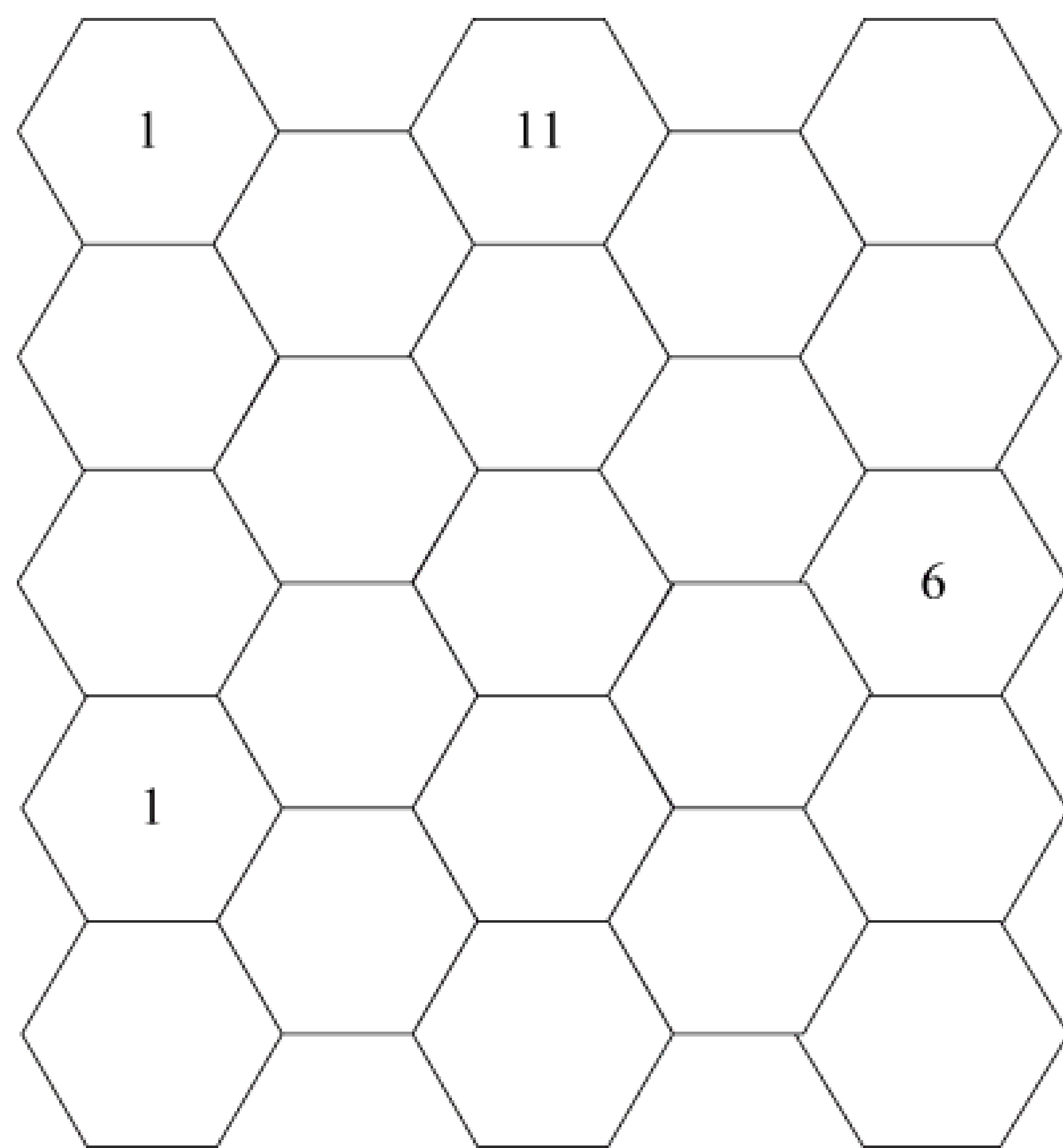
A. IEEE 802.11物理层将2.4GHz频段划分为14个独立的信道

B. 信道1的fc_1=2.412GHz,范围2.401~2.423GHz

C. 相邻的信道1与信道2之间频率没有重叠

D. 无线网络制造商一般采用信道1、6、11

4-7-6 按照2.4GHz信道复用的方法完成下图的信道规划。



4-7-7 以下不属于IEEE 802.11组网结构的是________。

A. BSS B. ESS C. WSN D. MBSS

4-7-8 以下关于BSS特点的描述中,错误的是________。

A. BBS是由一个基站AP与若干在逻辑上彼此关联的无线主机组成

B. BSS的覆盖范围限制在100m的范围内

C. BSS覆盖范围叫作基本服务区(BSA)

D. BSS形成了一个星形拓扑构型

4-7-9 以下关于ESS结构特点的描述中,错误的是________。

A. 多个BSS通过AP、Ethernet交换机与路由器接入到主干网构成分布式系统

(DS)

B. 多个 BSS 也可以通过无线网桥、无线路由器构成无线分布式系统(WDS)

C. AP 是无线主机访问分布式系统(DS)的接入设备

D. 主机向 AP 发送数据帧定义为"来自 DS"

4-7-10 以下关于 Ad hoc 网络特点的描述中,错误的是________。

A. 自组织与自修复　　B. 对等结构

C. 一跳路由　　D. 动态拓扑

4-7-11 以下关于 WMN 网络特点的描述中,错误的是________。

A. 混合型结构的网络

B. 多个 AP 之间形成 Ad hoc 网络

C. 每个无线 AP 都可以形成自己的 BSS

D. AP 增加了 IP 路由选择与自组织的功能

4-7-12 以下关于 BSS 中"冲突"现象的描述中,错误的是________。

A. 主机要将数据帧发送到基站 AP

B. AP 利用共享无线信道以"点对点"方式转发该帧

C. 如果有两个或两个以上无线主机同时发送就会发生"冲突"

D. IEEE 802.11 的 MAC 层协议就是要解决多个无线主机对共享无线信道的争用问题

4-7-13 以下关于 BSS 结构中对 SSID 与 BSSID 的描述,错误的是________。

A. SSID 是 BSS 的逻辑名

B. BSSID 是无线网卡 MAC 地址

C. BSSID 长度是 6 个字节(48 位)

D. SSID 与 BSSID 都可以由网络管理员分配

4-7-14 以下关于 IEEE 802.11 的 MAC 层访问控制协议特点的描述中,错误的是________。

A. 无争用服务系统的中心是基站——无线接入点(AP)

B. MAC 层分布协调功能 DCF 对应争用的服务

C. MAC 层点协调功能 PCF 对应无争用服务

D. PCF 提供的是"尽力而为"的服务

4-7-15 以下关于 Ethernet 与 Wi-Fi 的 MAC 特点描述中,错误的是________。

A. Ethernet 节点在总线空闲时立即发送帧

B. Wi-Fi 节点在监测到信道空闲后不是立即发送帧

C. Ethernet 节点在"冲突窗口"内没有检测出冲突就确认发送成功

D. Wi-Fi 节点根据退避算法执行之后是否出现冲突来判断此次发送是否成功

4-7-16 以下关于 802.11 帧间间隔的描述中,错误的是________。

A. 从发送一帧后到发送下一帧需要间隔的时间叫作帧间间隔

B. 帧间间隔的长短取决于发送帧的类型

C. 低优先级的帧等待的时间长

D. 高优先级的帧等待的时间短

4-7-17 对正确接收的数据帧进行确认的 MAC 协议是________。

A. CDMA　　B. CSMA　　C. CSMA/CD　　D. CSMA/CA

4-7-18 以下关于802.11发送与接收帧过程的描述中,错误的是________。

A. 发送主机的物理层根据接收到的信号强度来判断是否有主机发送数据信号

B. 信道空闲时,若等待一个DIFS时间间隔后信道仍然空闲,则发送一帧

C. 目的主机正确接收帧,等待SIFS时间间隔后发送ACK确认帧

D. 源主机在任何时候,只要接收到ACK帧就说明发送成功

4-7-19 以下关于802.11的VCS与NAV机制特点的描述中,错误的是________。

A. 设置VCS与NAV的目的是主动避免发生冲突的概率

B. 主机发出一帧时在持续时间字段填入以μs为单位的值

C. 持续时间字段值表示在该帧发送结束还要占用信道的时间。

D. 其他主机接收到“持续时间”字段值小于自己的NAV值,则修改自己NAV值

4-7-20 以下关于CSMA/CA“冲突退避”概念的描述中,错误的是________。

A. 为了进一步减少出现冲突的概率,802.11设计了“冲突退避”方法

B. 可能有多个待发送的主机都检测到NAV=0时信道空闲

C. 可能多主机同时发送数据帧从而出现冲突

D. NAV值为0后立即执行“二进制指数退避算法”

4-7-21 以下关于802.11“二进制指数退避算法”特点的描述中,错误的是________。

A. 第i次退避时间计算公式为$[2^{2+i}-1]$

B. 二进制指数退避算法退避变量最大值$i_{max}=6$

C. $i=2$时可以在$[0,1,\cdots,16]$中随机地选择一个

D. 随机选择12,表示第2次出现冲突之后主动延时12个时间片

4-7-22 以下关于802.3与802.11MAC层协议区别的描述中,错误的是________。

A. 802.3协议能够保证发送帧只要不出现冲突就能够正确被接收

B. 802.11协议要求目的主机向源主机发送回ACK确认帧

C. 802.3的MAC协议属于“无连接不确认协议”

D. 802.11的MAC协议属于“停止等待协议”

4-7-23 802.11设备标出速率为300Mbps,那么提供给用户的吞吐量只能是________。

A. 300Mbps　　B. 250Mbps　　C. 200Mbps　　D. 100Mbps

4-7-24 假设:在802.11b的BSS中,AP只关联了主机A与主机B,以CSMA/CA方式工作。主机A用最长的2342B数据帧向主机B发送数据,AP以长度为14B的ACK帧进行确认。主机B不向主机A发送数据,并且不考虑其他控制帧与管理帧的交互。

计算:AP与主机A、主机B以11Mbps与1Mbps的速率交互时,主机A每秒钟发送的数据帧数与有效的数据传输速率。

4-7-25 以下关于802.11信标帧网络特点的描述中,错误的是________。

A. Ad hoc模式中AP周期性地发送信标帧

B. 无线主机从接收到的信标帧发现可用的基站AP

C. 信标帧为无线主机接入到AP提供了必要的配置信息

D. 无线主机从接收信标帧的时间戳中提取AP的时钟用于时钟同步

4-7-26 以下关于 802.11 主动扫描与被动扫描特点的描述中，错误的是________。

A. 无线主机在接入 AP 之前首先要发现可接入的 AP
B. 发现 AP 的方法可以是被动扫描或主动扫描
C. 被动扫描的主机要扫描信道与监听多个 AP 信标帧
D. 主动扫描是由主机向一个 AP 广播探测帧来实现的

4-7-27 以下关于 802.11 协议支持两种级别的链路认证的描述中，错误的是________。

A. 802.11 协议支持两种级别的链路认证：开放系统认证与共享密钥认证
B. 开放系统认证的主机与 AP 只交换链路认证"请求帧"与"应答帧"
C. 只有在"Wi-Fi Free"的情况下才使用开放系统认证
D. 共享密钥认证的 WEP 协议将取代 WAP 协议

4-7-28 以下关于无线主机与 AP 关联的描述中，错误的是________。

A. 关联只能由 AP 发起
B. 一个时刻一台无线主机只能与一个 AP 关联
C. 主机从原 AP 覆盖的范围移动到新的 AP 覆盖的范围需要执行"重关联"
D. AP 发现关联的无线主机信号消失时，采取超时机制来解除与无线主机的关联

4-7-29 以下关于 802.11 的 AP 接受主机关联问题的描述中，错误的是________。

A. 无线主机是否具有以最高传输速率通信的能力
B. AP 能否为申请关联的无线主机提供所需要的缓冲空间
C. 节能模式主机处于休眠状态时准备接受的数据帧都要缓存在 AP 上
D. AP 将根据"关联请求帧"中 "聆听间隔"的时间长短预测需要的缓冲空间大小

4-7-30 以下关于 802.11 的 ESS 漫游与重关联概念的描述中，错误的是________。

A. ESS 中主机漫游时首先要发送"解除关联帧"
B. 从一个 AP 到另一个 AP 的漫游叫作"二层漫游"
C. 无线主机可以与多个 AP 认证，但只和一个 AP 关联
D. 无线网卡一般是根据信号的质量来决定是否要启动漫游和重关联的过程

4-7-31 以下关于 802.11 中 RTS/CTS 预约模式的描述中，错误的是________。

A. 源主机在检测到信道空闲并退避一个 DIFS 后产生一个 RTS 帧
B. 目的主机接收到 RTS 帧且信道空闲时发送一个 CTS 帧
C. 源主机接收到 CTS 帧并退避 SIFS 后发送数据帧
D. 信道的预约方法可以有效地解决隐藏主机问题

4-7-32 以下关于 802.11 数据帧结构的描述中，错误的是________。

A. 帧头长度为 30B
B. 数据字段长度在 0～2312B
C. 帧尾是由 2B 的帧校验字段组成
D. 帧头由帧控制、持续时间、地址 1～地址 3 与序号等组成

4-7-33 以下关于 802.11 帧控制字段的描述中，错误的是________。

A. 在管理帧中，类型与子类型值为 00 0000 表示探询请求帧
B. 在管理帧中，类型与子类型值为 00 1000 表示信标帧
C. 在控制帧中，类型与子类型值为 011011 表示 RTS 帧

D. 在数据帧中,类型与子类型值为10 0000表示数据帧

4-7-34 以下关于802.11帧控制字段中电源管理位的描述中,错误的是________。

A. 802.11协议在帧控制字段中设置1位的“电源管理”位

B. 在节能模式中,主机要关闭网卡,主机整体处于“休眠”状态

C. 在节能模式中,电源管理位为1表示主机在发送一帧后进入休眠状态

D. 在节能模式中,电源管理位为0表示主机在发送一帧后仍处于工作状态

4-7-35 以下关于802.11地址字段的描述中,错误的是________。

A. 协议规定帧头的4个地址字段并不是都出现在所有的帧中

B. 在BSS中,数据帧从源主机经过AP转发时,将使用到3个地址

C. AP向源主机发送数据帧时,帧控制字段的“去往DS=1、来自DS=0”

D. 地址4只用于无线自组网Ad hoc中

4-7-36 以下关于802.11无线网卡MAC控制器功能的描述中,错误的是________。

A. 将待发送的主机数据封装成数据帧

B. 执行CSMA/CA算法发送帧比特序列

C. 按照协议要求实现控制帧与管理帧的各种功能

D. 无线通信加密算法与加密程序由主机操作系统完成

4-7-37 以下关于802.11无线网卡分类的描述中,错误的是________。

A. 按照协议标准可以分为802.11a、802.11 b、802.11g与802.11n等

B. 按照接口类型可以分为外置、内置与内嵌无线网卡等

C. 外置网卡进一步分为PCI、PAMCIA与USB网卡等

D. 笔记本计算机内置网卡集成了天线

4-7-38 以下关于802.11无线接入点AP设备的发展的描述中,错误的是________。

A. 第一代无线接入点AP可用于构成BSS无线局域网

B. 第二代无线接入点AP可用于构成ESS无线局域网系统

C. 第三代无线接入点AP可用于构成集中管理的统一无线网络系统

D. 无线接入点AP与无线路由器是相同的

4-7-39 以下关于802.11“双频多模”AP的描述中,错误的是________。

A. 802.11物理层标准的不同导致了不同标准的无线设备之间存在兼容性问题

B. “双频多模”解决的是主机在不同物理层标准的BSS区域漫游的问题

C. “双频”是指可支持2.4GHz与5GHz两种频率

D. “多模”是指可支持BSS与Ad hoc应用模式

4-7-40 以下关于802.11动态VLAN的描述中,错误的是________。

A. 动态VLAN是结合身份认证机制,将虚拟局域网技术引入Wi-Fi中

B. 实现在一个BSS中为有不同需求的用户提供区分服务的功能

C. 属于同一VLAN的无线主机都会获得相同的BSSID

D. 身份认证服务器将主机分配到不同的VLAN中

4-7-41 以下关于802.11统一无线网络的描述中,错误的是________。

A. 无线局域网控制器WLC以集中方式管理的大型无线网络系统

B. WLC执行无线接入点控制与配置CAPWAP协议

C. Auto-RF 增强系统对无缝漫游的支持能力

D. 统一无线网络中的 AP 称为胖 AP

4-7-42 以下关于 802.11 无线局域网控制器 WLC 功能的描述中，错误的是________。

A. 动态分配信道，优化 AP 位置的分布

B. 支持主机的二层和三层漫游

C. 动态地均衡客户端的负载

D. 有效地安全性管理

第二部分　同步练习答案与解析

4.1　局域网技术的发展与演变

4-1-1　分析：设计该例题的目的是加深读者对局域网拓扑结构类型与特点的理解。在讨论局域网拓扑结构的类型与特点时，需要注意以下几个主要问题：

(1) 由于局域网设计目标是覆盖一个公司、一所大学、一幢办公大楼的“有限地理范围”，因此它的基本通信机制与广域网完全不同，从存储转发方式改变为共享介质与交换方式。

(2) IEEE 802.2 标准定义的共享介质局域网有以下三类：带有冲突检测的载波侦听多路访问(CSMA/CD)方法的总线型局域网、令牌总线(Token Bus)方法的总线型局域网、令牌环(Token Ring)方法的环形局域网。

(3) 总线型局域网的主要特点是：

- 所有节点都通过网卡连接到作为公共传输介质的总线上。
- 总线通常采用双绞线或同轴电缆作为传输介质。
- 所有节点都可以通过总线发送或接收数据，但是一段时间内只允许一个节点通过总线发送数据。当一个节点通过总线以“广播”方式发送数据时，其他节点只能以“收听”方式接收数据。
- 由于总线作为公共传输介质为多个节点共享，就可能出现同一时刻有两个或以上节点通过总线发送数据的情况，因此会出现冲突(collision)而造成传输失败。因此，每个节点什么时候能够获得发送数据帧的机会是不确定的。

(4) 介质访问控制方法是指控制多个节点利用公共传输介质发送和接收数据的方法。介质访问控制是所有“共享介质”类型局域网都必须解决的问题。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

4-1-2　分析：设计该例题的目的是加深读者对令牌总线工作原理的理解。在讨论令牌总线工作原理时，需要注意以下几个主要问题：

(1) 在令牌总线网中，节点通过环接口连接成逻辑环形。IEEE 802.4 标准定义了总线拓扑的令牌总线介质访问控制方法与相应的物理规范。

(2) 令牌总线是一种在总线拓扑中利用“令牌”(token)作为控制节点访问公共传输介质的确定型介质访问控制方法。在采用令牌总线方法的局域网中，任何一个节点只有在取得令牌后才能使用共享总线去发送数据。令牌是一种特殊结构的控制帧，用来控制节点对

总线的访问权。

(3) 由于协议规定了一个节点持有令牌的最大时间,因此节点两次获得令牌的最大时间间隔是确定的,因此令牌总线是一种确定型的介质访问控制方法,这一点是它与传统的Ethernet随机型介质访问控制方法最大的不同。

(4) 令牌总线协议比较复杂,需要完成大量的环维护工作。

(5) 令牌总线方法有以下几个主要特点:

① 介质访问延迟时间有确定值。

② 通过令牌协调各节点之间的通信关系,各节点之间不会发生冲突,在重负载情况下信道的利用率高。

③ 支持优先级服务。

从以上分析中可以看出,D对令牌总线特点的描述是错误的。

答案:D。

4-1-3 分析:设计该例题的目的是加深读者对令牌环网工作原理的理解。在讨论令牌环网时,需要注意以下几个主要问题:

(1) 在令牌环网中,节点通过环接口连接成物理环形。IEEE 802.5标准定义了令牌环介质访问控制方法与相应的物理规范。

(2) 令牌是一种特殊的MAC控制帧。令牌帧中有一位标志令牌的忙/闲。当环正常工作时,令牌总是沿着物理环单向逐站传送,传送顺序与节点在环中排列的顺序相同。

(3) 令牌环的控制方式具有与令牌总线相似的特点:环中节点访问延迟确定,适用于重负载环境,支持优先级服务。令牌环控制方式的缺点主要是:环维护复杂,实现较困难。

从以上分析中可以看出,A的描述是错误的。

答案:A。

4-1-4 分析:设计该例题的目的是加深读者对IEEE 802参考模型的理解。在讨论802参考模型时,需要注意以下几个主要问题:

(1) 802.1标准:定义了局域网体系结构、网络互联,以及网络管理与性能测试。

(2) 802.2标准:定义了逻辑链路控制LLC子层功能与服务。

(3) 目前主要的IEEE 802标准是:

① 802.3标准——定义CSMA/CD总线介质访问控制子层与物理层标准。

② 802.11标准——定义无线局域网访问控制子层与物理层的标准。

③ 802.15标准——定义近距离个人无线网络访问控制子层与物理层的标准。

④ 802.16标准——定义宽带无线局域网访问控制子层与物理层的标准。

从以上分析中可以看出,802.1标准定义了局域网体系结构、网络互联,以及网络管理与性能测试,物理层标准分别包括在802.11、802.15、802.16等标准中。

因此,D是错误的。

答案:D。

4-1-5 分析:设计这道习题的目的是加深读者对802.3协议特点的理解。

由于以太网的CSMA/CD算法执行的是一种分布式控制方法,访问共享总线的各个节点自主地决定发送帧的时间,在出现冲突时各自解决下一步什么时候再发送的问题,并且对已发送的帧,只要不发生冲突就认为是发送成功,MAC协议对发送帧是否出错不做处理,

如果出现帧丢失，也由高层协议去解决。

因此，以太网的 CSMA/CD 算法提供的是无连接不可靠服务。A 的描述是正确的。

答案：A。

4-1-6 分析：传播时延带宽积是评价网络传输性能的指标之一，设计该例题的目的是加深读者对传播延时带宽积概念的理解，以及不同条件下传播时延带宽积的比较。

(1) 图 4-1 给出了传输介质上正在传播的比特数的示意图。由于信号从发送节点传播到接收节点的传播延时与传输介质的长度 D，以及信号在传输介质中的传输速度 V 相关，即 $T_c = D/V$。

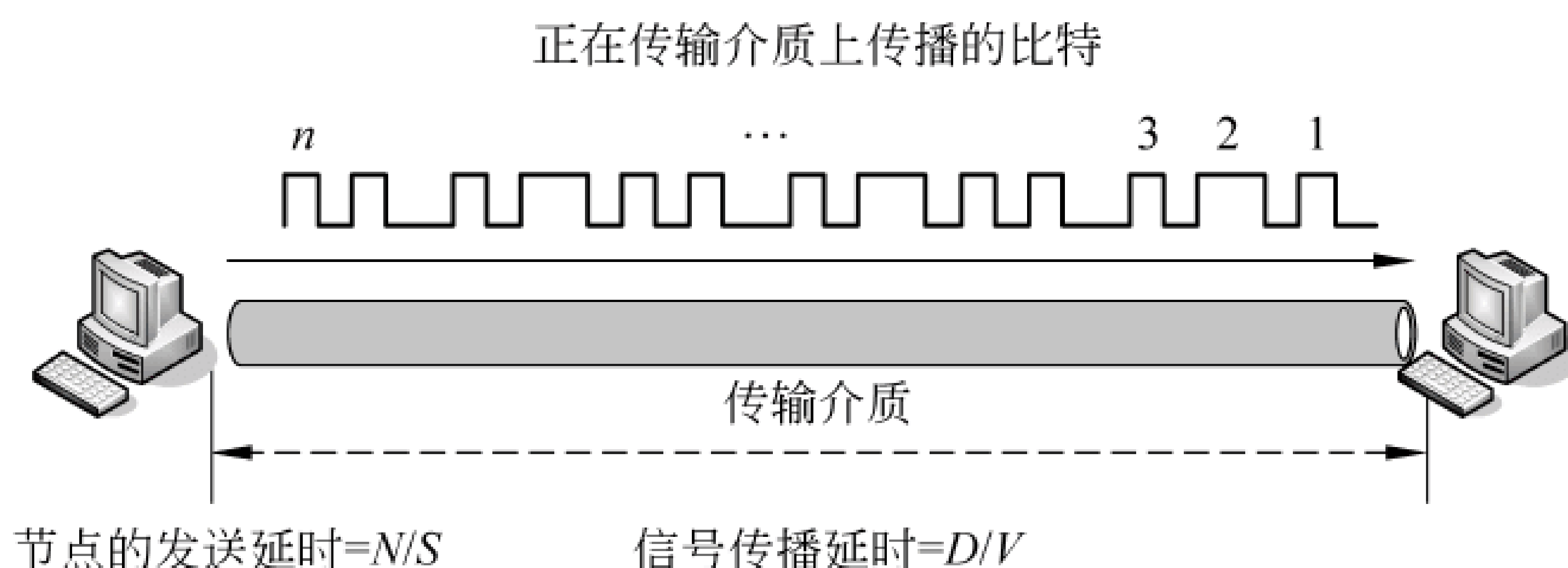


图 4-1 传输介质上正在传播的比特数示意图

(2) 如果发送节点发送速率为 S，那么在 T_c 时间出现在传输介质上的比特数 n 应该等于

$$n = S \times D/V$$

(3) 传输介质上正在传播的比特数与节点发送速率 S、传播延时相关，是衡量网络性能的参数之一，也称作“以比特为单位的链路长度”或“传播延时带宽积”。

计算：

(1) 传输介质长度：$D_1 = 0.1$m(网卡)；

① 发送速率 $S_1 = 1$Mbps；

传播延时 $T_{c1} = 0.1/2.3 \times 10^8 = 4.35 \times 10^{-10}$(s)

传播延时带宽积 $n = 1 \times 10^6 \times 4.35 \times 10^{-10} = 4.35 \times 10^{-4}$(bit)

② 发送速率 $S_1 = 10$Gbps；

传播延时 $T_{c1} = 0.1/2.3 \times 10^8 = 4.35 \times 10^{-10}$(s)

传播延时带宽积 $n = 1 \times 10^{10} \times 4.35 \times 10^{-10} = 4.35$(bit)

(2) 传输介质长度：$D_2 = 100$m(局域网)；

① 发送速率 $S_2 = 1$Mbps；

传播延时 $T_{c2} = 100/2.3 \times 10^8 = 4.35 \times 10^{-7}$(s)

传播延时带宽积 $n = 1 \times 10^6 \times 4.35 \times 10^{-7} = 0.435$(bit)

② 发送速率 $S_2 = 10$Gbps；

传播延时 $T_{c2} = 100/2.3 \times 10^8 = 4.35 \times 10^{-7}$(s)

传播延时带宽积 $n = 1 \times 10^{10} \times 4.35 \times 10^{-7} = 4.35 \times 10^3$(bit)

(3) 传输介质长度：$D_3 = 100$km(城域网)；

① 发送速率 $S_3 = 1$Mbps；

传播延时 $T_{c3}=1\times10^5/2.3\times10^8=4.35\times10^{-4}$(s)

传播延时带宽积 $n=1\times10^6\times4.35\times10^{-4}=4.35\times10^2$(bit)

② 发送速率 $S_3=10$Gbps;

传播延时 $T_{c3}=1\times10^5/2.3\times10^8=4.35\times10^{-4}$(s)

传播延时带宽积 $n=1\times10^{10}\times4.35\times10^{-4}=4.35\times10^6$(bit)

(4) 传输介质长度:$D_4=5000$km(广域网);

① 发送速率 $S_4=1$Mbps;

传播延时 $T_{c4}=5\times10^6/2.3\times10^8=2.17\times10^{-2}$(s)

传播延时带宽积 $n=1\times10^6\times2.17\times10^{-2}=2.17\times10^4$(bit)

② 发送速率 $S_4=10$Gbps;

传播延时 $T_{c4}=5\times10^6/2.3\times10^8=2.17\times10^{-2}$(s)

传播延时带宽积 $n=1\times10^{10}\times2.17\times10^{-2}=2.17\times10^8$(bit)

答案:如表4-1所示。

表4-1 传输介质长度、传输延时与传播延时带宽积

传输介质长度	传输延时(s)	传播延时带宽积(b)	
		速率=1Mbps	速率=10Gbps
0.1m	4.35×10^{-10}	4.35×10^{-4}	4.35
100m	4.35×10^{-7}	0.435	4.35×10^3
100km	4.35×10^{-4}	4.35×10^2	4.35×10^6
5000km	2.17×10^{-2}	2.17×10^4	2.17×10^8

4-1-7 分析:设计该例题的目的是加深读者对以太网技术发展趋势的理解。在讨论以太网技术发展趋势时,需要注意以下几个主要问题:

(1) 速率更高。

从1980年第一个速率为10Mbps的以太网标准出现之后的30多年中,高速以太网沿着100Mbps、1Gbps、10Gbps、40Gbps到100Gbps的步伐一步步地前进。2013年IEEE又成立了802.3bs工作组,研究速率达到400Gbps的下一代以太网标准与技术。

(2) 应用更广。

高速以太网与光以太网、城域以太网技术的发展,使得以太网的应用从局域网逐步扩大到城域网与广域网,正在向覆盖范围越来越广的方向发展;同时从组建办公环境的局域网,向组建近距离、高吞吐量、低延时的大型高性能计算机系统、存储区域网、云计算平台等后端计算机机房网络的方向发展;工业以太网正在广泛应用于工业自动化领域,成为工业4.0发展的重要支撑技术。

(3) 与无线局域网兼容。

IEEE在802.11无线局域网标准制定过程中,一直保持与802.3标准的以太网兼容,因此,有人将无线局域网Wi-Fi称为"无线以太网"。

(4) 更环保。

2000年有一份研究报告指出:从100Mbps到1Gbps的以太网端口耗电约4W。如果

美国1.6亿台接入以太网的计算机在网络空闲时进入低功率模式，一年可以节约2.4亿美元的电费。2010年9月，IEEE发布的802.3az支持“Energy Efficient以太网，EEE”的标准。

因此，A对802.3bs工作组研究的下一代以太网速率的描述是错误的。

答案：A。

4.2 Ethernet技术的研究与发展

4-2-1 分析：设计该例题的目的是加深读者对以太网工作原理的理解。在讨论以太网工作原理时，需要注意以下几个主要问题：

(1) 以太网的MAC子层采用CSMA/CD方法。

(2) CSMA/CD发送流程可以概括为：

- 先听后发。
- 边听边发。
- 冲突停止。
- 延迟重发。

第一步，载波侦听过程。

每个以太网主机利用总线发送数据时，首先需要侦听总线是否空闲，总线此时处于空闲状态，则这个主机就可以“启动发送”。第一步可以总结为“先听后发”。

第二步，冲突检测方法。

载波侦听并不能完全消除冲突。发送主机必须在发送过程中进行“冲突检测”。第二步可以总结为“边听边发”。

第三步，冲突停止。

如果在发送数据过程中检测出冲突，发送主机要进入停止发送数据，转入随机延迟后重发的流程。发送流程的第三步可以总结为“冲突停止”。

第四步，延迟重发。

延迟重发的第一步是发送“冲突加强信号”，然后加入随机延迟阶段，以太网协议规定一个帧的最大重发次数为16。如果重发次数$n \leqslant 16$，则允许主机随机延迟再重发。第四步可以总结为“延迟重发”。

因此，C的描述是错误的。

答案：C。

4-2-2 分析：设计这道题目的目的是加深读者对CSMA/CD“冲突域”与“冲突窗口”的理解。

(1) 在以太网协议标准中，规定的冲突窗口长度为51.2μs。

(2) 以太网的数据传输速率为10Mbps，冲突窗口的51.2μs可以发送512bit(64B)数据。

(3) 64B是以太网的最小帧长度。这意味着当一台主机发送一个最小帧，或一个帧的前64个字节时没有发现冲突，则表示该主机已经获得总线发送权，并可以继续发送后续的字节。

(4) 冲突窗口又称为“争用期(contention period)”。

从以上分析中可以看出，D的描述是错误的。

答案：D。

4-2-3 分析：设计这道习题的目的是加深读者对CSMA/CD工作原理的理解。求解这个问题需要注意以下几个问题。

第一问：

已知条件：第一，在采用CSMA/CD算法的局域网中，如果总线长度为1000m，电磁波传播速度为2×10^8m/s。主机A与B分别连接在总线的两端。第二，出现冲突。

求主机A与主机B能够检测到冲突发生的最短时间与最长时间。

分析：

冲突产生的原因：连接在局域网中的两台主机A和B相距距离为D，电磁波传播的深度为V，那么主机A向B发送一帧数据要经过D/V传播延时之后，主机B才可能接收到这个数据帧。在这传播延时的时间内，主机B并不知道主机A已发送数据，它就有可能也向主机A发送数据。当出现这种情况时，主机A与主机B的发送就发生“冲突”。这里存在两种极端的情况。

第一种情况是主机A与主机B同时发生一帧信号，那么这两个帧就会在$D/2$的位置碰撞，发生冲突，帧发送经过$D/2V$时间后出现冲突(如图4-2所示)。然后发生冲突的帧仍然要向主机A与主机B传播。再通过$D/2$距离之后，同样经过$D/2V$时间后分别被主机A、主机B检测到。这样，主机A、B同时发送帧，又同时检测到冲突的时间最短，为D/V。在这道题中，$D=1000$m，$V=2\times10^8$m/s，那么最短可以检测到冲突的时间为5μs。

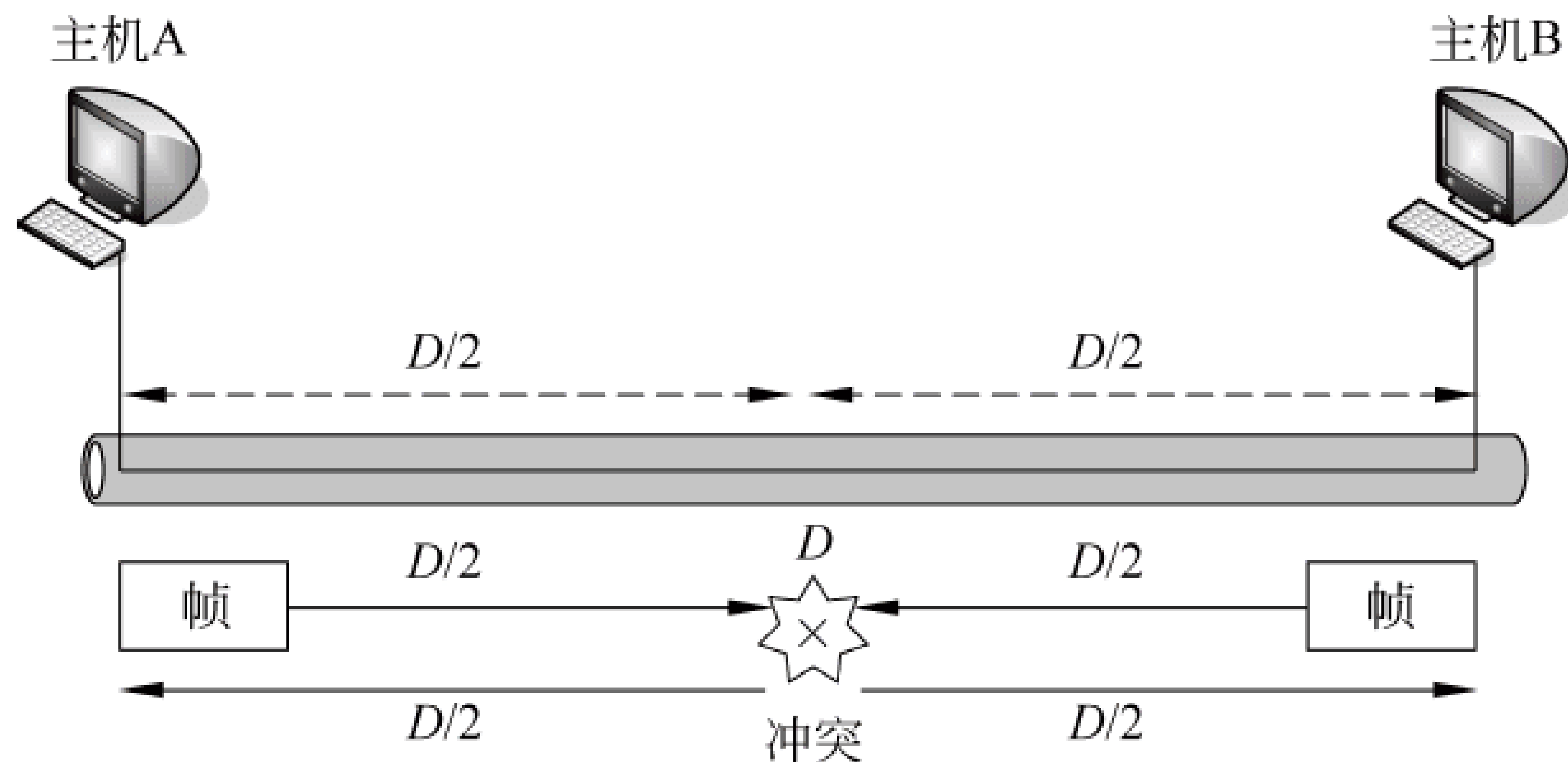


图4-2 最短可以检测到冲突的时间的冲突情况

第二种情况是主机A向主机B发送了数据，在数据信号快要达到主机B时，主机B也发送了数据，此时冲突发生。等到冲突的信号传送回主机A时，已经过两倍的传播延迟$2D/V$。在两倍传播延迟的时间内，冲突帧可以传遍整个网段。整个网段上连接的所有计算机都应该检测到冲突(如图4-3所示)。

因此，最长可以检测到冲突的时间就是冲突窗口的时间。本题中为10μs。

第二问：

已知条件：

- 没有出现冲突；
- 主机A总是以最大帧长度(1518B)向主机B发送数据帧；
- 主机B每接收到一个数据帧立即向主机A发送64B的确认帧；
- 主机A在接收到确认帧之后才可以发送下一帧。

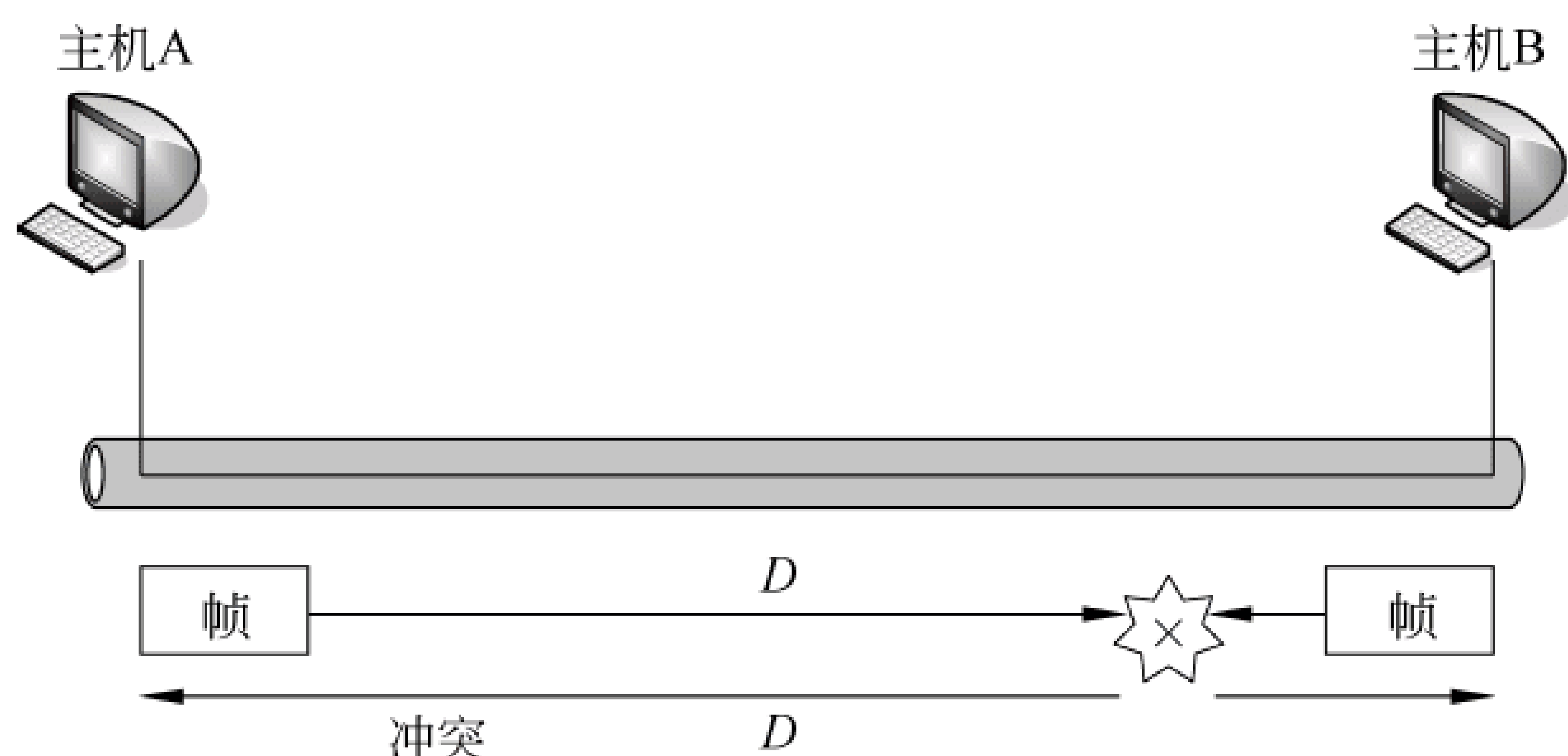


图 4-3　最长可以检测到冲突的时间的冲突情况

求主机 A 的有效数据传输速率：

（1）主机 A 发送 1 数据帧所用时间，即发送延时：$t_1=1518\times8/10^7\approx1.2144(\text{ms})$

（2）主机 B 发送 1 确认帧所用时间，即发送延时：$t_2=64\times8/10^7\approx0.0512(\text{ms})$

（3）帧信号出一端到另一端的传播延时：$t_3=1000/2\times10^8\text{m/s}=5\mu\text{s}=0.005\text{ms}$

（4）主机 A 发送 1 数据帧传播到主机 B，主机 B 发送 1 确认帧再传播到主机 A 的时间：

$$T_0=t_1+t_2+2t_3=1.2144+0.0512+0.01=1.2756(\text{ms})$$

T_0 为主机 A 发送 1 数据帧的时间。

因此，主机 A 每秒钟发送的数据帧数 $N=1/T_0=1000/1.2756\approx784$（帧/秒）。有效发送速率 $S=1500\times8\times784\approx9.41(\text{Mbps})$

答案：（1）最短可以检测到冲突的时间为 5μs；最长可以检测到冲突的时间为 10μs。

（2）主机 A 每秒钟发送 784 帧，有效发送速率约等于 9.41Mbps。

4-2-4　分析：设计这道习题的目的是加深读者对以太网"冲突窗口"原理的理解。

（1）设置"冲突窗口"的目的是：保证所有连接在共享总线上的节点都能够在这个时间内检测到总线上是否发生冲突。冲突窗口值等于 $2D/V$。

（2）最小帧长度与总线长度、发送速率之间的关系：最短帧长度为 $L_{\min}$，主机发送速率为 S，发送短帧所需要的时间为 $L_{\min}/S$。要求发送一个最短帧的时间都要超过冲突窗口的时间，即

$$L_{\min}/S\geqslant2D/V$$

那么，总线长度与最小帧长度、发送速率之间的关系为

$$D\leqslant VL_{\min}/2S$$

可以根据总线长度、发送速率与电磁波传播速度，估算出最小帧长度。

（3）计算条件：

① 光速在同轴电缆中的传播速度 $V=2\times10^8\text{m/s}$。

② 网卡的发送速率为 1Gbps（1×10^9bps）。

③ 最小帧长度减小 800bit。

求解的问题：连接在同轴电缆两端的计算机之间的距离是增加还是减小？变化量为多少米？

设：最初的最小帧长度为 L_1，那么对应的总线长度 $D_1=V\times L_1/2S$。

减小后的最小帧长度为 L_2，那么对应的总线长度 $D_2=V\times L_2/2S$。

两次总线长度之差：

$$\Delta D=D_1-D_2=V\times L_1/2S-V\times L_2/2S=V\times(L_1-L_2)/2S$$

已知：最小帧长度减小600bit，即：$L_1-L_2=600(\text{bit})$，$\Delta D>0$，即 $D_1>D_2$

将此值代入到上式，得：

$$\Delta D=2\times10^8\times600/2\times10^9=60(\text{m})$$

答案：当网卡发送速率不变，减小最小帧长度600bit，对应的总线长度也要相应减少；减少的值为60m。

4-2-5 分析：关于截止二进制指数后退延迟算法的讨论，需要注意以下几个问题：

(1) 以太网协议规定一个帧的最大重发次数为16。如果重发次数 $n\leqslant16$，则允许主机随机延迟再重发。

(2) CSMA/CD后退延迟算法是截止二进制指数后退延迟：算法：$\tau=2^k\times R\times a$。

其中，τ 为重新发送所需的后退延迟的时间，a 是冲突窗口值，R 是随机数。如果一台主机需要计算后退延迟时间，则需要以其地址为初始值产生一个随机数 R。

(3) 为了避免延迟过长，截止二进制指数后退延迟算法限定作为二进制指数 k 的范围，定义了 $k=\min(n,10)$。最大可能延迟时间为1023个时间片。

(4) 以太网使用的CSMA/CD方法被定义为一种随机争用型介质访问控制方法。CSMA/CD方法可以有效控制多主机对共享总线的访问，方法简单并且容易实现。

因此，D的描述是错误的。

答案：D。

4-2-6 分析：设计该例题的目的是加深读者对以太网帧的理解。在讨论以太网时，需要注意以下几个主要问题：

(1) Ethernet V2.0标准与IEEE 802.3标准的以太网帧结构是有区别的。Ethernet V2.0规范是在DEC、Intel与Xerox公司合作研究的以太网协议的基础上改进而成，因此有些文献中将Ethernet V2.0帧结构称为DIX帧结构。IEEE 802.3标准对Ethernet帧结构也作出了规定，我们通常称为802.3帧。DIX帧和802.3帧结构是有差异的。

(2) DIX与IEEE 802.3帧结构的差异主要表现在以下两点：

第一，前导码部分。

① DIX帧的前8B是前导码，每个字节都是10101010。接收电路通过提取曼彻斯特编码的自含时钟，实现收发双方的比特同步。

② 802.3帧规定7B前导码由56位的10101010…10101010比特序列组成，之后有一个结构为10101011的帧前定界符。如果将前导码与帧前定界符结合在一起看，在62位101010…1010比特序列后出现11。在这个11比特之后才是Ethernet帧的目的地址字段。

第二，类型字段与长度字段。

① DIX帧规定了一个2B的类型字段。类型字段表示高层网络层所使用的协议类型。例如，类型字段值等于0x0800，表示网络层使用IPv4协议；类型字段值等于0x8106，表示地址解析ARP协议；类型字段值等于0x86DD，表示网络层使用IPv6协议。

② 802.3帧规定该字段为“长度字段”。数据字段是网络层发送的数据部分。由于帧最小长度为64B，帧头部分长度为18B(6B的目的地址、6B的源地址字段、2B的长度字段、4B的帧校验字段)，因此数据字段最小长度为64－18＝46(B)。数据字段最大长度为

1500B,因此数据字段长度为46～1500B,不是固定长度的。从这个角度看,设置“长度字段”是合理的。

从以上分析中可以看出,C的描述是错误的。

答案：C。

4-2-7 分析：设计该例题的目的是加深读者对IEEE 802.3中“长度/协议字段”定义的理解。在讨论IEEE 802.3对“长度/协议字段”定义时,需要注意以下几个问题：

(1) 由于Ethernet V2.0标准已经广泛应用,所以IEEE 802.3标准在之后的修订中拿出了一个折中的方案,将2B定义的“长度字段”改为“长度/协议字段”。同时表示长度或协议是不矛盾的。

(2) 以太网数据字段最大长度为1500B,加上帧头部分长度为18B,帧的最大长度小于1518B。如果用十六进制表示,长度字段值一定小于0x0600。而IEEE定义的“协议字段值”最小为0x0800(IP协议)。

(3) 以太网的MAC层可根据需要发送两种帧,可以表示上层协议的类型,也可以表示帧长度。这样,接收端MAC层可以根据该字段的值来解释该字段表示的意义。这样就可以很好地解决IEEE 802.3标准与Ethernet V2.0标准之间存在的差异问题。

从以上分析中可以看出,B的描述是错误的。

答案：B。

4-2-8 分析：设计该例题的目的是加深读者对以太网的CRC校验范围的理解。

在讨论以太网帧的CRC校验时,需要注意以下几点：

(1) 帧采用32位的CRC校验。

(2) CRC校验的范围是：目的地址、源地址、长度、LLC。

因此,A的描述是错误的。

答案：A。

4-2-9 分析：设计这道习题的目的是帮助读者加深对Ethernet“冲突加强”特点的理解。在讨论Ethernet的“冲突加强”特点时,需要注意以下几个问题：

(1) 如果在发送数据过程中检测出冲突,发送主机要进入停止发送数据、随机延迟后重发的流程。

(2) 随机延迟重发的第一步是发送“冲突加强干扰序列信号(或冲突加强信号)”。

(3) 冲突加强干扰序列信号长度规定为32bit。

(4) 发送冲突加强信号的目的是：确保有足够的冲突持续时间,使网中的所有主机都能检测出冲突存在,并立即丢弃冲突帧,减少由于冲突浪费的时间,提高信道利用率。

从以上分析中可以看出,B的描述是错误的。

答案：B。

4-2-10 分析：设计该例题的目的是加深读者对以太网接收过程的理解。在讨论以太网接收过程时,需要注意以下几个问题：

(1) 如果一个主机成功利用总线发送数据帧,则其他主机都应该处于接收状态。

(2) 当某个主机的以太网卡完成一帧数据接收后,首先要判断接收的帧长度。如果接收帧长度小于规定的帧最小长度,则表明冲突发生,应该丢弃该帧,主机重新进入等待接收状态。

(3) 以太网通信协议属于无连接不确认/重传的协议,发送出现冲突,其他节点不发送出错重传通知。

因此,D的描述是错误的。

答案:D。

4-2-11 分析:设计该例题的目的是加深读者对以太网卡功能与结构的理解。在讨论以太网卡功能与结构时,需要注意以下几个问题:

(1) 以太网卡应该包含:

① 发送与接收信号的收发器。

② 曼彻斯特编码与解码器。

③ 以太网数据链路控制。

④ 组帧与拆帧软件。

⑤ 与主机的接口。

(2) 以太网卡的功能覆盖了802.3协议的MAC子层与物理层。

因此,以太网卡不包含网卡驱动程序,A的描述是错误的。

答案:A。

4-2-12 分析:设计该例题的目的是加深读者对以太网物理地址的理解。

以太网物理地址是一个重要概念。理解以太网物理地址,需要注意以下几个问题:

(1) 对以太网物理地址的管理方法。

① 以太网物理地址就是MAC地址,长度为48bit,称为扩展的唯一标识符EUI-48。

② 48位的以太网物理地址允许分配的地址数量应该为2^{47}个。

③ 为了统一管理以太网的物理地址,保证每块以太网网卡的地址是唯一的,IEEE注册管理委员会(RAC)为每个网卡生产商分配以太网物理地址的前3字节,即机构唯一标识符(OUI)。后面3字节由网卡的生产商自行分配。

(2) 以太网物理地址的表示方法。

① 当网卡生产商获得一个前3个字节地址分配权后,它可以生产的网卡数量是2^{24}(16 777 216)块。

② 物理地址可以写为02-01-00-2A-10-C3或0201002A10C3。

(3) 以太网物理地址的唯一性。

① 在网卡生产过程中,网卡的物理地址写入网卡的只读存储器中。

② 网卡的物理地址都是不变的,并且在全球是唯一的。

(4) 关于全局管理/本地管理(G/L)位与单播/多播(I/G)位的规定。

IEEE RAC初期讨论以太网物理地址分配方法时,由于考虑到有人可能不愿意向IEEE RAC购买OUI,因此规定以太网物理地址的第一字节的最低的第二位为G/L(Global/Local)位。

① G/L=0表示本地管理的物理地址,用户可以任意分配,但是不能够保证这个地址是全球唯一的。

② G/L=1表示全局管理的物理地址。所有向IEEE RAC购买OUI的以太网卡的物理地址G/L=1。

③ 所有以太网卡的MAC地址都是G/L=1的全局管理的地址,保证在全世界都是唯一的。

因此,C 的描述是错误的。

答案:C。

4-2-13 分析:设计该例题的目的是加深读者对以太网物理层标准命名方法的理解。在讨论以太网物理层标准命名方法时,需要注意以下几个问题:

(1) 标准的以太网的物理层命名方法是 IEEE 802.3 X Type-Y Name。其中:

① X 表示数据传输速率,单位为 Mbps。

② Y 表示网段的最大长度,单位为 100m。

③ Type 表示传输方式是基带还是频带。

④ Name 表示局域网的名称。

例如,IEEE 802.3 10BASE-T 表示传输速率为 10Mbps、基带传输、使用的双绞线的以太网物理层标准。

(2) 当以太网的速率提高之后,所使用的传输介质可能从非屏蔽双绞线、屏蔽双绞线变成多模或单模光纤,新的物理层标准的命名方法仍然保持不变。

因此,D 的描述是错误的。

答案:D。

* **4-2-14**

1. 分析:这是一个估算局域网吞吐量的题目。在计算时需要注意以下几个因素:

(1) 关于以太网帧最大帧长度与最小帧长度时应该考虑两种情况。第一种情况是对于接收端来说,它不考虑以太网帧的 8B 帧前定界符。帧前定界符起到接收端与发送双方的同步作用,实际上接收到的数据帧部分不包括 8B 帧前定界符。对于接收端来说,它考虑的以太网帧最大帧长度是 1518B,而最小帧长度是 64B。第二种情况是对发送端来说,它需要考虑 8B 的帧前定界符,实际在发送端发送的帧长度应该包括帧前定界符。因此,实际发送的以太网帧最大帧长度与最小帧长度都应该加上 8B 的帧前定界符,即发送的以太网帧的最大帧长度为 1526B 与最小帧长度 72B。

(2) 802.3 标准规定帧与帧之间需要留一个帧间间隔时间,数值为 9.6μs。

(3) 以太网的传输速率为 10Mbps。

2. 计算:

(1) 传输速率为 10Mbps,带宽利用率为 50%,考虑帧间间隔。

① 传输速率为 10Mbps,带宽利用率为 50%时,实际可利用的传输速率为 5Mbps。

发送的以太网帧的最大帧长度为

$$1526\text{B}=1526\times 8=12208(\text{bit})$$

最小帧长度为

$$72\text{B}=576(\text{bit})$$

② 发送最大帧长度每帧需要的时间为

$$\Delta t_1=9.6\times 10^{-6}+12208/5\times 10^{6}=9.6+2441.6=2451.2(\mu\text{s})$$

那么,每秒钟可以发送最大长度的帧数为

$$1/2451.2\times 10^{-6}\approx 408$$

③ 发送最小帧长度每帧需要的时间为

$$\Delta t_2=9.6\times 10^{-6}+576/(5\times 10^{6})=(9.6+114.2)\times 10^{-6}=124.8(\mu\text{s})$$

那么,每秒钟可以发送最小长度的帧数为

$$1/(124.8\times10^{-6})\approx8013$$

(2) 传输速率为100Mbps。

① 传输速率为100Mbps,带宽利用率为50%时,实际可利用的传输速率为50Mbps。

② 发送最大帧长度每帧需要的时间为

$$\Delta t_3=9.6\times10^{-6}+12208/(5\times10^7)=(9.6+244.16)\times10^{-6}=253.8(\mu s)$$

那么,每秒钟可以发送最大长度的帧数为

$$1/(253.8\times10^{-6})\approx3940$$

③ 发送最小帧长度每帧需要的时间为

$$\Delta t_4=9.6\times10^{-6}+576/(5\times10^7)=9.6+11.52=21.12(\mu s)$$

那么,每秒钟可以发送最大长度的帧数为

$$1/(21.12\times10^{-6})\approx47349$$

答案:

(1) 当传输速率为10Mbps时,每秒钟可以发送最大长度帧数约为408个,发送最小长度帧数约为8013个。

(2) 当传输速率为100Mbps时,每秒钟可以发送最大长度帧数约为3940个,发送最小长度帧数约为47 349个。

* **4-2-15** 计算:

(1) 传播时间 $\Delta t=L/V=1000/(2\times10^8)=5(\mu s)$

(2) 冲突窗口 $2\Delta t=10(\mu s)$

(3) 最短帧长度 $L_{min}=1\times10^7\times10\times10^{-6}=100(bit)=12.5(B)$

答案:最短帧长度为100bit或12.5B。

* **4-2-16** 分析:

(1) CSMA/CD后退延迟算法是截止二进制指数后退延迟(truncated binary exponential backoff)算法。该算法可以表示为 $\tau=2^k\times R\times a$。其中,τ 为重新发送所需的后退延迟时间,a 为冲突窗口值,R 为随机数。如果一个节点需要计算后退延迟时间,则需要以其地址为初始值产生一个随机数 R。冲突窗口 a 值是确定的。

(2) 为了避免延迟过长,截止二进制指数后退延迟算法限定作为二进制指数 k 的范围,它定义了 $k=\min(n,10)$。如果重发次数 $n<10$,则 k 取值为 n;如果重发次数 $n\geq10$ 时,则 k 取值为10。第 n 次重发延迟分布在0与 $[2^{\min(n,10)}-1]$ 个时间片内,最大可能延迟时间为1023个时间片。

(3) 以太网协议规定一个帧的最大重发次数为16。如果重发次数超过16,则认为线路故障,进入"冲突过多"结束状态。如果重发次数 $n\leq16$,则允许节点随机延迟再重发。当冲突次数超过16时,表示发送失败,放弃该帧的发送。

计算:

(1) 重传失败的概率

重传失败的概率:$P_i=2^{-k},k=\min[i,10]$

① $k=1,P_{i1}=2^{-1}=0.5$

② $k=2,P_{i2}=2^{-2}=0.25$

③ $k=3, P_{i3}=2^{-3}=0.125$

(2) 一个节点成功传输数据之前的平均重传次数。

第 i 次传输成功的概率

$$\begin{aligned} P[\text{第 } i \text{ 次传输成功}] &= P[\text{第 1 次传输失败}]P[\text{第 2 次传输失败}]\cdots \\ &\quad P[\text{第 } i-1 \text{ 次传输失败}]P[\text{第 } i \text{ 次传输成功}] \\ &= 2^{-1}\times 2^{-2}\times\cdots\times 2^{-(i-1)}\times(1-2^{-1}) \end{aligned}$$

$$\begin{aligned} \text{平均重传次数} &= 1\times(1-2^{-1})+2\times 2^{-1}\times(1-2^{-2}) \\ &\quad +3\times 2^{-1}\times 2^{-2}\times(1-2^{-3})+\cdots \\ &= 1+2^{-1}+2^{-3}+2^{-6}+\cdots \\ &\approx 1.64 \end{aligned}$$

答案：

(1) 重传失败的概率：

① 第 1 次失败概率 $P_{i1}=0.5$

② 第 2 次失败概率 $P_{i2}=0.25$

③ 第 3 次失败概率 $P_{i3}=0.125$

(2) 平均重传次数约等于 1.64。

* **4-2-17** 分析：

(1) CSMA/CD 是以太网用来解决多节点共享共用总线的控制算法。以太网的 MAC 技术从纯 ALOHA、时间片 ALOHA 到载波侦听多路访问 CSMA，再到带有冲突检测的载波侦听多路访问 CSMA/CD 方法的演化过程。

(2) 在发生冲突的情况下成功发送一帧的过程如图 4-4 所示。图中 Δt 是信号在传输介质上从一端传播到另一端所需要的传播时间。$2\Delta t$ 就是 CSMA/CD 中定义的冲突窗口值。

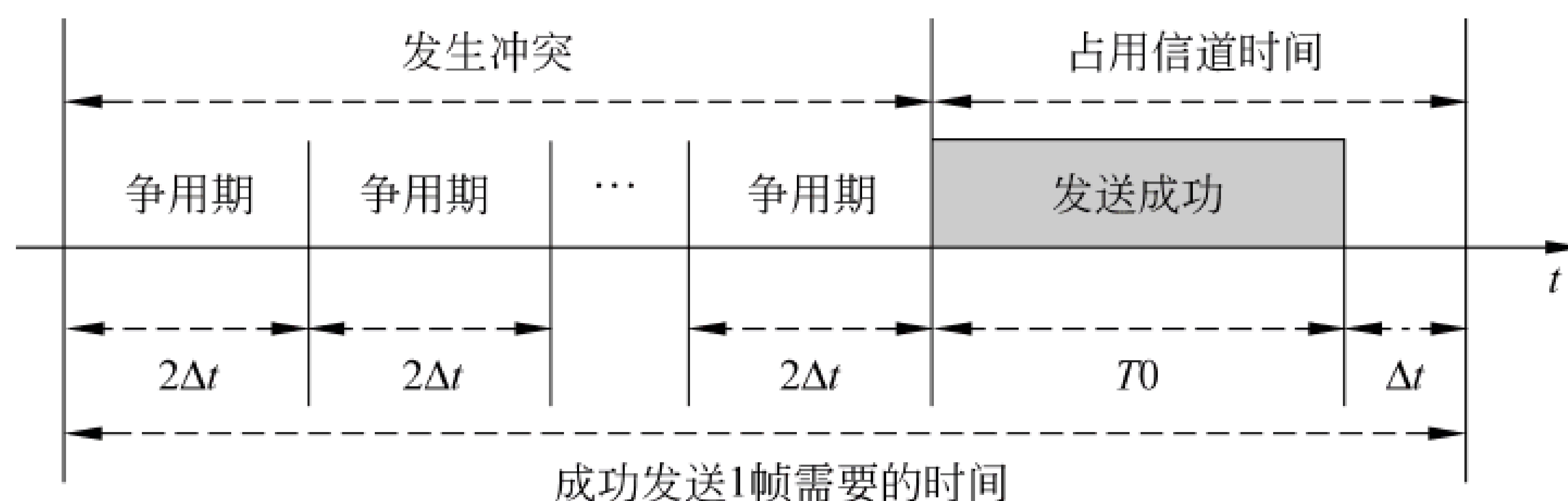


图 4-4 在发生冲突的情况下成功发送 1 帧的过程示意图

(3) 对于图 4-4，其中有几点需要说明：

① 图 4-4 只是一个示意图，因为它没有考虑二进制指数退避算法的作用。如果考虑二进制指数退避算法，那么冲突解决期间争用期长度是不等和非线性的。

② T_0 是发送延时，$T_0=L/S$，其中 L 为帧长度，S 为节点发送速率。

③ 发送一帧占用的时间应该为 $T_0+\Delta t$，因为必须考虑信号在总线上的传播时间。在 $T_0+\Delta t$ 之后，其他节点才可以进入争用阶段。

(4) 在上题的基础上，可以进行以下讨论：

① Ethernet 的信道的利用率。

$$a = \Delta t/T_0 = (D/V)/(L/S) = DS/VL \tag{4-1}$$

提高信道利用率就必须增大 T_0，或减小 Δt。也就是说，总线长度不能够太长，帧长度不能够太短。

② 考虑一种理想情况：节点发送不存在冲突，那么信道的极限利用率可以达到

$$a_{max} = T_0/(T_0 + \Delta t) = 1/(1 + a) \tag{4-2}$$

③ 当考虑节点数比较多时，信道的利用率可以达到

$$a_{max} \approx 1/(1 + 4.44a) \tag{4-3}$$

④ 根据平均帧长度与数据传输速率，可以得出每秒钟可以发送的帧数；根据信道利用率就可以估算每秒钟可能成功的帧数。

计算：

(1) 总线长度为4km，发送速率为5Mbps。

已知：节点数为100，平均帧长度为1000bit，传播延时为5μs/km。

① $T_0 = 1000/(5\times10^6) = 200(\mu s)$

② $\Delta t = 5\times4 = 20(\mu s)$

③ $a = 20/200 = 0.1$

④ $a_{max} \approx 1/(1+4.44\times0.1) \approx 0.69$

⑤ 每秒钟发送的帧数 $N = (5\times10^6)/(1\times10^3) = 5\times10^3$

⑥ 每秒钟可能成功发送的帧数 $n = (5\times10^6)\times0.69 = 3450$

(2) 总线长度为1km，发送速率为5Mbps。

已知：节点数为100，平均帧长度为1000bit，传播延时为5μs/km。

① $T_0 = 1000/(5\times10^6) = 200(\mu s)$

② $\Delta t = 5\times1 = 5(\mu s)$

③ $a = 5/200 = 2.5\times10^{-2}$

④ $a_{max} \approx 1/(1+4.44\times2.5\times10^{-2}) \approx 0.90$

⑤ 每秒钟发送的帧数 $N = (5\times10^6)/(1\times10^3) = 5\times10^3$

⑥ 每秒钟可能成功发送的帧数 $n = (5\times10^3)\times0.90 = 450$

(3) 总线长度为1km，发送速率为10Mbps。

已知：节点数为100，平均帧长度为1000bit，传播延时为5μs/km。

① $T_0 = 1000/(10\times10^6) = 100(\mu s)$

② $\Delta t = 5\times1 = 5(\mu s)$

③ $a = 5/100 = 0.05$

④ $a_{max} \approx 1/(1+4.44\times0.05) \approx 0.82$

⑤ 每秒钟发送的帧数 $N = (10\times10^6)/(1\times10^3) = 1\times10^4$

⑥ 每秒钟可能成功发送的帧数 $n = (1\times10^4)\times0.82 = 8200$

答案：

(1) 当总线长度为4km、发送速率为5Mbps，每秒钟可能成功发送的帧约为3450。

(2) 当总线长度为1km、发送速率为5Mbps，每秒钟可能成功发送的帧约为450。

(3) 当总线长度为1km、发送速率为10Mbps，每秒钟可能成功发送的帧约为8200。

* **4-2-18** 分析：

(1) Ethernet 的信道利用率：$a=\Delta t/T_0=(D/V)/(L/S)=DS/VL$

本题中 $a=DS/VL=(100\times1\times10^9)/(2\times10^8\times L)=500/L$。

(2) 信道利用率可以达到：

$$a_{max}\approx1/(1+4.44a)$$

(3) 根据 a_{max} 值与数据传输速率 S 值，可以计算出不同以太网帧长度的总线最大吞吐率 $P=a_{max}\times S$。

计算：

(1) 帧长度 $L_1=512\text{B}$

$a_1=DS/VL=500/(512\times8)\approx0.122$

$a_{max1}=1/(1+4.44\times0.122)=1/1.54\approx0.649$

$P_1=0.649\times1\times10^9=649(\text{Mbps})$

(2) 帧长度 $L_2=1500\text{B}$

$a_2=DS/VL=500/(1500\times8)\approx0.042$

$a_{max2}=1/(1+4.44\times0.042)=1/1.185\approx0.844$

$P_2=0.844\times1\times10^9=844\text{M}(\text{bps})$

(3) 帧长度 $L_3=64000\text{B}$

$a_3=DS/VL=500/(64000\times8)\approx0.001$

$a_{max3}=1/(1+4.44\times0.001)=1/1.0044\approx0.996$

$P_3=0.996\times1\times10^9=996\text{M}(\text{bps})$

答案：

(1) 当帧长度 $L_1=512\text{B}$ 时，总线最大吞吐率约为 649Mbps。

(2) 当帧长度 $L_2=1500\text{B}$ 时，总线最大吞吐率约为 844Mbps。

(3) 当帧长度 $L_3=64000\text{B}$ 时，总线最大吞吐率约为 996Mbps。

(4) 从以上计算数据中可以看出，当总线长度、发送速率不变时，帧长度越长，总线的数据吞吐率也就越高。

4.3 交换式局域网与虚拟局域网技术

4-3-1 分析：设计这道习题的目的是加深读者对局域网交换机工作原理的理解。

以太网交换机是链路层的设备，因此在决定转发策略时使用的是目的 MAC 地址。

答案：A。

4-3-2 分析：设计该例题的目的是加深读者对交换式局域网的理解。在讨论交换式局域网时，需要注意以下几个主要问题：

(1) 交换式局域网的核心设备是局域网交换机。局域网交换机利用集成电路交换芯片在多个端口之间同时交换数据，以实现多对连接在不同端口主机之间帧的并发传输。

(2) 交换机的“端口号/MAC 地址映射表”记录端口号与节点 MAC 地址的对应关系。交换机的交换控制机构根据“端口号/MAC 地址映射表”(简称为端口转发表或地址表)的对应关系，找出对应的输出端口号。

(3) 交换机建立和维护端口转发表的基本方法是“地址学习”。“地址学习”是交换机通过检查帧的源地址与帧进入交换机的端口号之间的对应关系，来不断获取端口转发表数据

的方法。

(4) 交换机交换方式主要有三种类型：直接交换、改进的直接交换与存储转发交换方式。

① 在直接交换方式中，交换机只要接收并检测到目的地址字段，立即将该帧转发出去，而不进行差错校验。帧出错检测任务由节点主机完成。

② 改进的直接交换方式则将二者结合起来，在接收到 Ethernet 帧的前 64B 后，判断帧头字段是否正确，如果正确就转发出去。

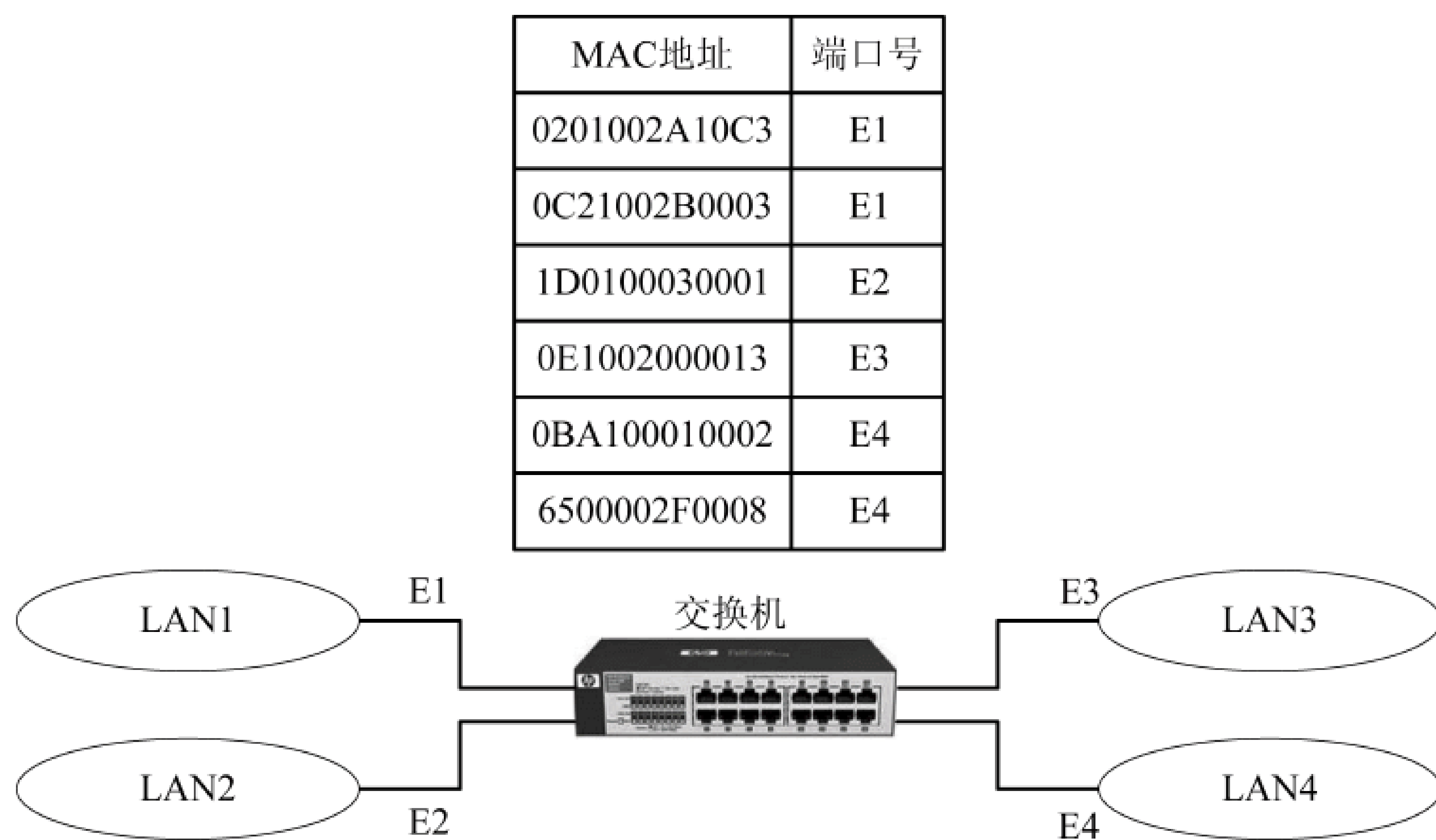
③ 在存储转发(store and forward)方式中，交换机首先要完整地接收帧，并进行差错检测。如果接收帧正确，则根据帧目的地址选择对应的输出端口号，然后转发出去。

从以上分析中可以看出，B 关于地址学习的描述是错误的。

答案：B。

4-3-3 分析：设计这道习题的目的是加深读者对交换机工作原理的理解。

从图 4-5 可以看出，用 Ethernet 交换机的 E1～E4 的 4 个端口连接了 LAN1～LAN4，显然，交换机的转发表正处于"学习"阶段。



MAC地址	端口号
0201002A10C3	E1
0C21002B0003	E1
1D0100030001	E2
0E1002000013	E3
0BA100010002	E4
6500002F0008	E4

图 4-5　网络结构示意图

如果交换机从 E2 端口接收到一个帧之后，交换机要完成两项任务：一是通过学习去完善转发表，二是转发该帧。

(1) 交换机从 E2 端口接收到一个帧的源地址为 0010A13B5611，这个地址不在转发表中，那么交换机需要在转发表中增加"端口 E2"对应 MAC 地址为 0010A13B5611 的项。接收帧目的地址为 08BA0011206B，不在转发表中，交换机需要通过除去 E2 端口之外的 E1、E3、E4 端口转发出去。

(2) 交换机从 E2 端口接收到一个帧的源地址为 0010A13B5611，这个地址不在转发表中，那么交换机需要在转发表中增加"端口 E2"对应 MAC 地址为 0010A13B5611 的项。接收帧目的地址为 1D0100030001 在转发表中，对应的端口号为 E2。交换机在端口 E2 接收到这个帧，说明 MAC 地址为 0010A13B5611 的节点与 MAC 地址为 1D0100030001 的节点同在 LAN2 中。因此交换机不转发、丢弃该帧。

答案：

（1）交换机需要通过除去 E2 端口之外的 E1、E3、E4 端口转发出去。

（2）交换机不转发、丢弃该帧。

4-3-4 分析：设计该例题的目的是加深读者对 VLAN 概念的理解。在讨论 VLAN 概念时，需要注意以下几个主要问题：

（1）VLAN 并不是一种新型的局域网，而是局域网向用户提供的一种新的服务。

（2）VLAN 是建立在局域网交换技术的基础上。

（3）VLAN 以软件方式来实现逻辑工作组的划分与管理，逻辑工作组中的节点组成不受物理位置的限制。

（4）当一个节点从一个逻辑工作组转移到另一个逻辑工作组时，只需要简单地通过软件设定来改变逻辑工作组，而不需要改变它在网络中的物理位置。

（5）同一个逻辑工作组的节点可以分布在不同物理网段上，但它们之间的通信就像在同一物理网段上一样。

从以上分析中可以看出，A 关于 VLAN 性质的描述是错误的。

答案：A。

4-3-5 分析：设计该例题的目的是加深读者对 VLAN 概念的理解。在讨论 VLAN 概念时，需要注意：尽管基于交换机端口是静态 VLAN 划分最常用的方法，但是 VLAN 划分也可以根据交换机端口、MAC 地址、IP 地址与网络层协议来进行。

因此，A 的描述是错误的。

答案：A。

4-3-6 分析：设计该例题的目的是加深读者对 IEEE 802.1Q 协议的理解。在讨论 IEEE 802.1Q 协议时，需要注意以下几个主要问题：

（1）IEEE 802.1Q 用了 4B 的 VLAN 标识来扩展以太网帧结构。扩展标准的以太网帧结构包括 2B 的标记协议标识符 TPID 与 2B 的标记控制信息 TCI。

（2）标记协议标识符 TPID。

第一个字段是 2B 的标记协议标识符（TPID），表示该帧是 IEEE 802.1Q 协议扩展的以太网帧。TPID 取值为 0X8100（10000001 00000000）。

（3）标记控制信息 TCI。

第二个字段是 2B 的标记控制信息（TCI）。第二个字段 TCI 又分为：3bit 的优先级（priority）、1bit 的规范格式指示符（CFI）与 12bit 的 VLAN 标识符（VID）。

优先级（priority）可以将用户分为 8 个级别。规范格式指示符 CFI 表示该帧是否符合以太网规范。在以太网交换机中，该位总是被置 0。VLAN 标识符 VID 长度为 12bit，其中 0 与 4095 被保留。VID 取值在 1～4094 之间。

从以上分析中可以看出，C 关于扩展的 Ethernet 帧 TPID 取值的描述是错误的。

答案：C。

4.4 快速 Ethernet 的研究与发展

4-4-1 分析：设计该例题的目的是加深读者对快速以太网特点的理解。在讨论快速以太网时，需要注意以下几个主要问题：

(1) 快速以太网(Fast Ethernet,FE)标准是IEEE 802.3u。

(2) FE传输速率达到100Mbps,但是它保留着传统的10Mbps速率Ethernet的基本特征,即相同的帧格式与最小、最大帧长度等特征。这样做的目的是:局域网中可以同时存在10Mbps的传统以太网与100Mbps的快速以太网。那么,在局域网速率提升之后,只是在物理层出现了不同,高层软件不需要做任何变动。

(3) 802.3u标准定义了介质专用接口(MII),将MAC层与物理层分隔开。这样,物理层在实现100Mbps速率时使用的传输介质和信号编码方式的变化不会影响MAC子层。

(4) 目前,100BASE-T有三种物理层标准:100BASE-TX、100BASE-T4、100BASE-FX。

(5) 传统以太网工作在半双工模式。快速以太网除了可以提供半双工模式之外,也可以工作在全双工模式。在全双工模式下,网卡就必须通过两个通道、两对双绞线与交换机连接,其中一对双绞线用于发送数据,而另一对双绞线用于接收数据。全双工模式不存在争用问题,MAC层不需要采用CSMA/CD方法。

(6) 增加10Mbps与100Mbps速率自动协商功能。协议规定自动协商过程需要在500ms内完成。

从以上分析中可以看出,C关于介质专用接口的描述是错误的。

答案:C。

4-4-2 分析:设计该例题的目的是加深读者对GE技术特点的理解。在讨论GE特点时,需要注意以下几个主要问题:

(1) GE的传输速率达到了1000Mbps,但是它仍然保留着传统以太网的帧格式与最小、最大帧长度等特征。

(2) 802.3z标准定义了千兆介质专用接口(GMII),将MAC子层与物理层分隔开。这样,物理层实现1000Mbps速率时的传输介质和信号编码方式变化,不会影响MAC层。

(3) 目前流行的GE物理层标准主要有1000BASE-CX、1000BASE-T、1000BASE-SX、1000BASE-LX、1000BASE-LH。

(4) 1000BASE-CX使用两对屏蔽双绞线,双绞线最大长度为25m。1000BASE-ZX使用单模光纤,光纤最大长度为70km。

从以上分析中可以看出,A关于GE与传统以太网兼容性的描述是错误的。

答案:A。

4-4-3 分析:设计该例题的目的是加深读者对10GbE特点的理解。在讨论10GbE特点时,需要注意以下几个主要问题:

(1) 10GbE标准是IEEE 802.3ae。

(2) 10GbE保留着传统以太网的帧格式与最小、最大帧长度的特征。

(3) 10GbE只工作在全双工方式,例如在网卡与交换机之间使用两根光纤连接,分别完成发送与接收的任务,因此不再采用CSMA/CD协议,这就使10GbE的覆盖范围不受传统以太网的冲突窗口限制,因此传输距离只取决于光纤通信系统的性能。

(4) 10GbE定义了专用的介质专用接口(10GMII),将MAC层与物理层分隔开。这样,物理层在实现10Gbps速率时使用的传输介质和信号编码方式的变化不会影响MAC子层。

(5) 10GbE的应用领域已经从局域网,逐渐扩展到城域网与广域网的核心交换网中。

(6) 10GbE 的物理层协议分为两类：局域网物理层标准与广域网物理层标准。

(7) LAN PHY 标准根据所使用的传输介质分为光纤与双绞线两类。

(8) 实现 WAN PHY 标准的技术路线主要有两种：使用 SONET/SDH 光纤通道技术，直接采用光纤密集波分复用 DWDM 技术。

(9) 对于广域网应用，10GbE 如果使用光纤通道技术，10GbE 广域网物理层应符合光纤通道技术速率体系 SONET/SDH 的 OC-192/STM-64 的标准。OC-192/STM-64 的标准速率是 9.95328Gbps，而不是精确的 10Gbps。如果直接采用光纤波分复用 DWDM 技术，10GbE 速率保持为 10Gbps。

从以上分析中可以看出，B 关于 10GbE 工作模式的描述是错误的。

答案：B。

4-4-4 分析：设计该例题的目的是加深读者对 40GbE 与 100GbE 的理解。在讨论 40GbE 与 100GbE 时，需要注意以下几个主要问题：

(1) 城域网与广域网核心交换网的传输带宽面临着巨大挑战，现有的 10GbE 技术已经开始难以应对日益增长的需求，更高速率的 40Gbps 与 100Gbps 的快速以太网的研究与应用就很自然地提上了议事日程，并且出现从 10GbE 向 40GbE、100GbE 的平滑过渡的发展趋势。

(2) 40GbE 技术将会大量应用于 IDC、高性能计算机、高性能服务器集群与云计算平台。

(3) 100GbE 不是一个单项技术的研究，而是一系列技术的综合，其中包括相关技术标准、以太网技术、密集波分复用 DWDM 传输技术等多个方面。

(4) 100GbE 的 802.3ba 标准。

(5) 100GbE 仍然保留着传统以太网的帧格式与最小、最大帧长度的规定。

(6) 100GbE 物理接口主要有三种类型：短距离互联的 LAN 接口、中短距离互联的 LAN 接口，以及 10m 的铜缆接口和 1m 的系统背板互联技术。

从以上分析中可以看出，D 关于 100GbE 的 802.3ab 标准名称的描述是错误的。

答案：D。

4-4-5 分析：设计该例题的目的是加深读者对光以太网与城域以太网的理解。在讨论光以太网与城域以太网时，需要注意以下几个主要问题：

(1) 经过多年的发展，以太网技术发生了根本性变化。光以太网(Optical Ethernet)与城域以太网(Metro Ethernet)就是最有代表性的成果，它标志着以太网的应用已经从传统的局域网的范畴向城域网、广域网延伸。

光以太网与城域以太网的概念都是在 2000 年前后提出的。实际上，光以太网与城域以太网两者是密不可分的。但是，光以太网的概念偏重于技术，而城域以太网的概念更偏重于应用。

(2) 光以太网研究的核心思想是：利用光纤的巨大带宽资源与成熟、广泛应用的以太网技术，为网络运营商建造新一代的宽带城域网提供技术支持。

(3) 光以太网的设备和线路必须符合电信网络 99.999%的高运行可靠性。它要克服传统以太网的不足，具备以下特征：

- 能够根据终端用户的实际应用需求分配带宽，保证带宽资源充分、合理地应用。

- 具有认证与授权功能,用户访问网络资源必须经过认证和授权,确保用户和网络资源的安全及合法使用。
- 提供计费功能,能及时获得用户的上网时间记录和流量记录,支持按上网时间、用户流量或包月计费方式,支持实时计费。
- 支持 VPN 和防火墙,可以有效地保证网络安全。
- 支持 MPLS,具有一定的服务质量保证,提供分等级的 QoS 网络服务。
- 能够方便、快速、灵活地适应用户和业务的扩展。

因此,研究可运营的光以太网已经不是单一的技术研究,而是提出了城域以太网的解决方案。光以太网、城域以太网的发展将从根本上改变网络运营商规划、建设、管理思想。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

4.5 Ethernet 组网设备与组网方法

4-5-1 分析:设计该例题的目的是加深读者对集线器特征的理解。在讨论集线器特征时,需要注意以下几个主要问题:

(1) 集线器(Hub)是以太网的节点连接设备之一,它是对总线型结构的一种改进。

(2) 集线器作为以太网中的中心连接设备时,所有节点通过非屏蔽双绞线与集线器连接。

(3) 这种以太网在物理结构上是星形结构,但在逻辑上仍然是总线型结构,在 MAC 层仍然采用 CSMA/CD 介质访问控制方法。

(4) 当集线器接收到某个节点发送的帧时,它立即将数据帧通过广播方式转发到其他端口。

(5) 普通的集线器都提供两种类型的端口:一类是用于连接节点的 RJ-45 端口,这类端口数可以是 8、12、16、24 等;另一类端口是用来级联的 RJ-45、AUI、BNC 或 F/O 端口,这类端口通常称为向上连接端口。

(6) 从节点到集线器的非屏蔽双绞线最大长度为 100m,利用集线器向上连接端口级联可以扩大局域网的覆盖范围。单一集线器结构适用于小型工作组规模的局域网。如果需要连网的节点数超过单一集线器的端口数时,通常需要采用多集线器的级联结构,或是采用可堆叠式集线器。

从以上分析中可以看出,B 的描述是错误的。

答案:B。

4-5-2 分析:

(1) 连接到一台以太网集线器的所有节点共享一个冲突域,如果以太网集线器的带宽为 S,接入的节点数为 N,那么每个节点可以得到的平均带宽为 S/N。

(2) 如果以太网交换机的端口带宽为 10Mbps,交换机可以在端口之间建立并发连接,每个端口可以独享 10Mbps 带宽。

计算:

(1) 10 个节点连接到一台 10Mbps 的 Ethernet 集线器,那么每个节点可以得到的平均

带宽为1Mbps。

(2) 10个节点连接到一台100Mbps的Ethernet集线器,那么每个节点可以得到的平均带宽为10Mbps。

(3) 10个节点连接到一台10Mbps的Ethernet交换机,那么每个节点可以得到的平均带宽为10Mbps。

答案：在以上三种情况下,每个节点的平均带宽分别为1Mbps、10Mbps与10Mbps。

4.6 局域网互联与网桥的基本工作原理

4-6-1 分析：设计该例题的目的是加深读者对网桥概念的理解。在讨论网桥的概念时,需要注意以下几个主要问题：

(1) 网桥的功能是实现局域网的互联。

(2) 网桥能够互联采用不同数据链路层协议、不同传输介质与不同传输速率的网络。

(3) 网桥以接收、存储、地址过滤与转发的方式实现互联网络之间的通信。

(4) 网桥需要互联网络在数据链路层以上采用相同的协议。

(5) 网桥可以分隔两个网络之间的广播通信量,有利于改善互联网络的性能与安全性。

从以上分析中可以看出,A关于网桥互联层次的描述是错误的。

答案：A。

4-6-2 分析：设计该例题的目的是加深读者对网桥基本分类的理解。在讨论网桥基本分类时,需要注意以下几个主要问题：

(1) 网桥利用路由表实现不同网段之间帧转发的过程。网桥最重要的工作是构建和维护路由表。

(2) 网桥按照其路由表的建立方法分为两类：透明网桥与源路由网桥。这两种网桥标准分别由IEEE 802.1与802.5分委员会制定。

(3) 透明网桥由各个网桥自己来决定路由选择,局域网上的各节点不负责路由选择,网桥对于互联局域网的各节点来说是透明的。

(4) 源路选网桥由发送帧的源节点负责路由选择。

从以上分析中可以看出,网桥处理的是局域网数据链路层的物理地址与端口号的映射关系,A混淆了物理地址与IP地址。

答案：A。

4-6-3 分析：设计该例题的目的是加深读者对透明网桥与生成树算法的理解。在讨论透明网桥与生成树算法时,需要注意以下几个主要问题：

(1) 透明网桥由各个网桥来决定路由选择。透明网桥的标准是IEEE 802.1d。透明网桥的最大优点是容易安装,是一种即插即用设备。

(2) 透明网桥的路由表要记录三个信息：站地址、端口与时间。透明网桥刚刚连接到局域网时,其路由表是空的。当它接收到一个帧时,它将记录收到的帧的源MAC地址、帧进入该网桥的端口号以及帧进入该网桥的时间。然后,它将该帧向所有的其他端口转发,帧进入网桥的端口除外。网桥在这样的转发过程中,逐渐地将其路由表建立起来。

(3) 生成树算法。为了避免在多个网桥互联的系统中出现环形结构,透明网桥使用了

一个生成树算法。为了建造生成树,首先必须选出一个网桥作为生成树的根。该算法的结果是建立起从每一个局域网到根网桥的唯一路径。该过程由生成树算法软件自动运行产生;在拓扑结构改变时,将更新计算生成树。该过程将保证网络中任何两个设备之间只有一个通路,创建了一个逻辑上无环路的网络拓扑结构。

从以上分析中可以看出,A的描述是错误的。

答案:A。

4-6-4 分析:设计该例题的目的是加深读者对源路由网桥的理解。在讨论源路由网桥时,需要注意以下几个主要问题:

(1) IEEE 802.5分委员会制定了源路由(source routing)网桥标准。源路由网桥由发送帧的源节点负责路由选择。

(2) 源路由网桥假定每个节点在发送帧时,都已经清楚地知道发往各个目的节点的路由,因此在发送帧时将详细的路由信息放在帧头部。

(3) 为了发现适合的路由,源节点以广播方式向目的节点发送一个用于探测的发现帧(discovery frame)。发现帧将在整个通过网桥互联的局域网中沿着所有可能的路由传送。当这些发现帧到达目的节点时,就沿着各自的路由返回源节点。如果有超过一条的路径,源节点将选择经过的中间网桥跳数最少的路径。

(4) 发现帧的另一个作用是帮助源节点确定整个网络可以通过的帧的最大长度。

从以上分析中可以看出,源节点选择的是经过中间网桥跳数最少的路径,而与路由器无关。因此,B的描述是错误的。

答案:B。

4-6-5 分析:

设计这道习题的目的是帮助读者加深对生成树协议的理解。在讨论生成树协议时,需要注意以下几个主要问题:

(1) 生成树协议自动控制局域网系统的拓扑,形成一个无环路(loop-free)的逻辑结构,使得任意两个网桥或交换机之间、任意两个局域网之间只有一条有效的帧传输路径。

(2) 生成树协议执行的第一步是选择一个网桥为根网桥。无环路的逻辑结构是从根网桥出发,构成通向每个网桥与局域网的树状结构。

(3) 网络管理员需要为每个网桥分配一个优先级。优先级加上MAC地址就构成了网桥标识。选择根网桥的方法是先比较网桥的优先级,如果优先级相同,则选择MAC地址数最小的作为根网桥。

这道题做出了一个简化:在STP协议执行过程中,只比较网桥的ID值。因此,可以通过比较ID值,以ID值小为优先级高的原则选择根网桥与转发路径。

解答:

(1) 选择B1为根网桥。

(2) 凡是出现环路的位置,通过选择ID值小的为互联网桥,断开ID值大的网桥。

这样就可以形成图4-6所示的无环路的逻辑结构。

答案:图4-7是执行STP协议之后形成的无环路网络互联结构图。

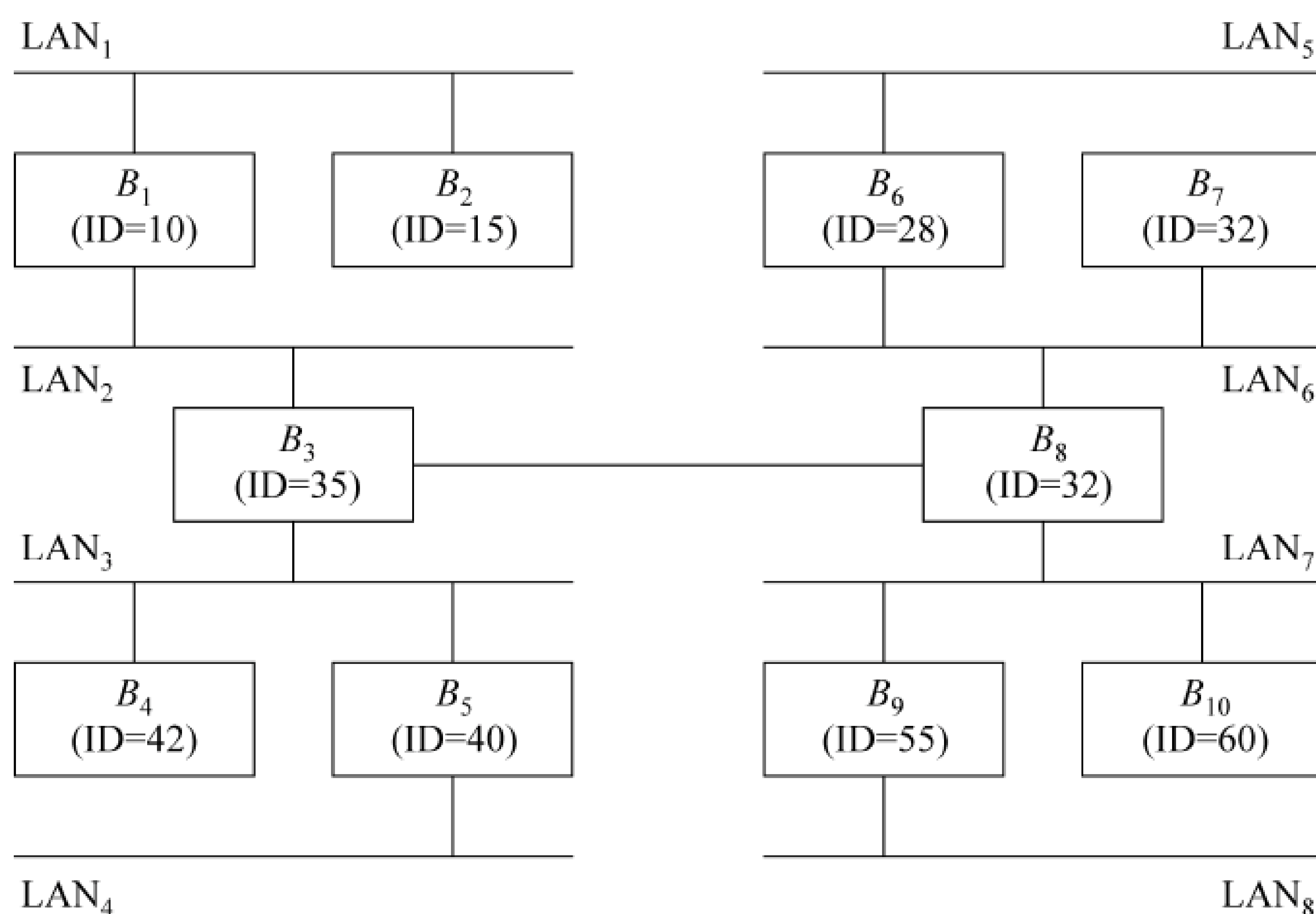


图 4-6　无环路网络互联结构

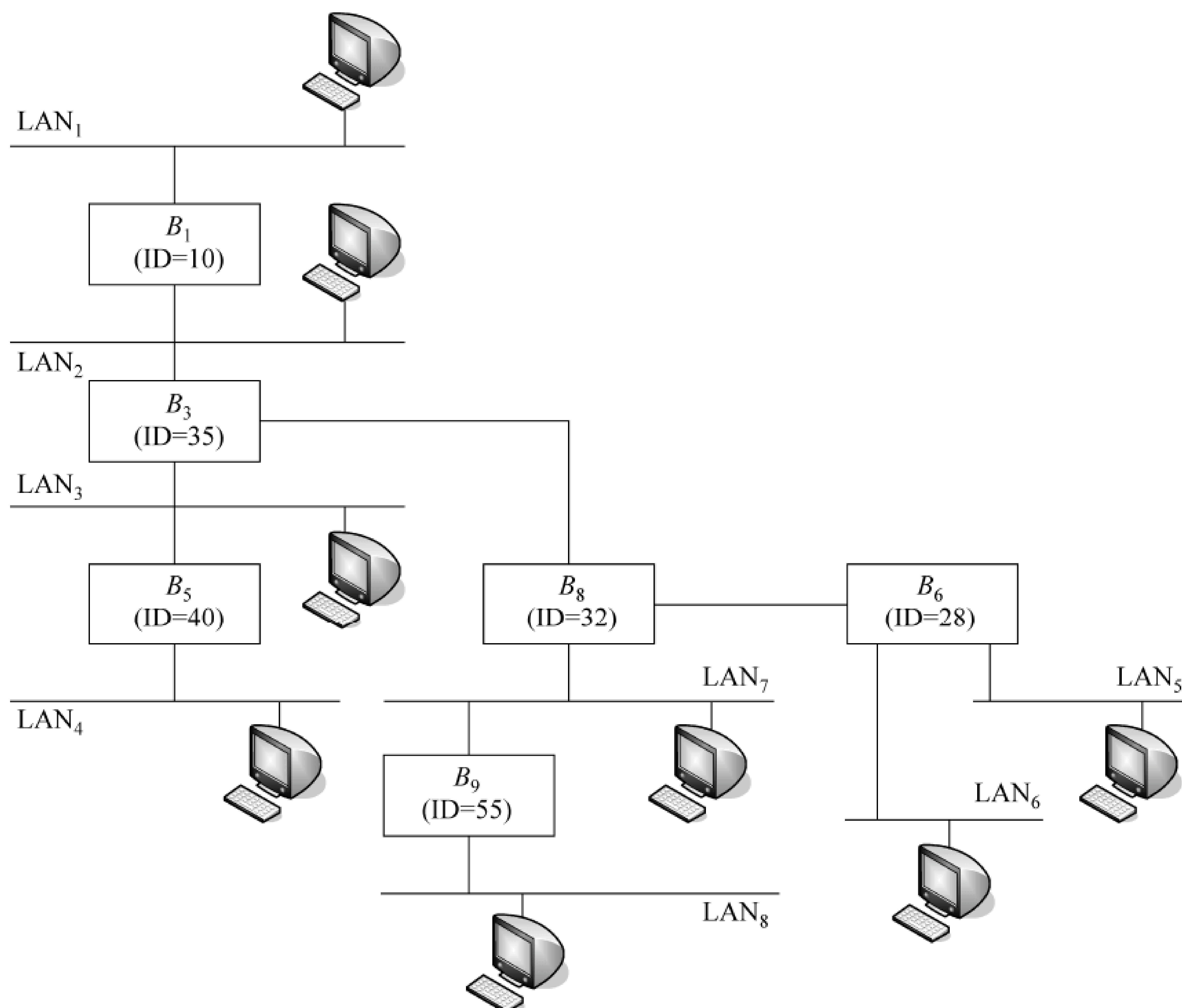


图 4-7　执行 STP 协议后的无环路网络互联结构

4.7　无线局域网

4-7-1　分析：IEEE 802.11n 标准具有以下几个特点：

(1) 802.11n 可以工作在 2.4GHz 与 5GHz 两个频段，速率最高可以达到 600Mbps。

(2) 802.11n 采用了智能天线技术,通过多组独立的天线组成天线阵列,可以动态地调整天线的方向图,达到减少噪声干扰、提高无线信号的稳定性、扩大覆盖范围的目的。一台802.11n 接入点的覆盖范围可以达到几平方公里。

(3) 802.11n 采取了软件无线电技术,解决了不同工作频段、不同信号调制方式带来的系统不兼容问题。802.11n 不但能与 802.11a/b/g 标准兼容,而且可以实现与无线城域网802.16 标准的兼容。

正是由于 802.11n 具有以上特点,因此,802.11n 已经成为“无线城市”建设中的首选技术,并且大量进入家庭与办公室环境中。

从以上分析中可以看出,A 的描述是错误的。

答案:A。

4-7-2 分析:802.11ac 与 802.11ad 修正草案被称为“千兆 Wi-Fi 标准”,其特点如下:

(1) 2011 年发布的 802.11ac 草案是工作频段为 5GHz、传输速率为 1Gbps 的 Wi-Fi 标准。

(2) 2012 年发布的 802.11ad 草案抛弃了拥挤的 2.4GHz 与 5GHz 频段,定义了工作频段在 60GHz、传输速率为 7Gbps 的 Wi-Fi 标准。

(3) 这些技术都考虑了与 802.11a/b/g/n 标准兼容的问题。

(4) 由于 802.11ad 使用的工作频段在 60GHz,因此它的信号覆盖范围比较小,更适合于家庭高速 Internet 接入应用。

从以上分析中可以看出,B 的描述是错误的。

答案:B。

4-7-3 分析:802.11b 协议规定了 11Mbps、4.5Mbps、2Mbps 与 1Mbps 共 4 种传输速率。

从以上分析中可以看出,C 的描述是错误的。

答案:C。

4-7-4 分析:设计这道习题的目的是帮助读者进一步加深对 802.11 协议动态速率调整 DRS 技术特点的理解。

(1) 一种 IEEE 802.11 协议标准会规定若干个传输速率,例如 802.11b 协议规定了11Mbps、4.5Mbps、2Mbps 与 1Mbps 共 4 种传输速率。这就要求符合 802.11b 标准的接入点 AP 允许主机的无线网卡在建立关联时,协商选择其中一种速率进行通信。

(2) 在无线主机移动过程中,无线网卡和 AP 的距离在变化,主机无线网卡接收到的信号质量随之改变,这就会造成无线网卡与无线接入点 AP 之间的传输速率随距离增大而降低的现象。当无线主机距离 AP 近(例如在 10m 以内)时,无线网卡可以采用 11Mbps 传输速率;当距离达到为 75m 时,信号幅度下降、信噪比降低,帧传输质量下降,则传输速率降为4.5Mbps;当距离达到 250m 时,就需要进一步降为更低的 2Mbps 或 1Mbps。这个过程称为动态速率调整(Dynamic Rate Switching,DRS)。

(3) 动态速率调整 DRS 是移动主机中的无线网卡发送数据的速率随着接收到发送方AP 的信号质量下降而下调的一种反馈控制机制。设计 DRS 的目标是通过协调传输距离与数据传输速率的矛盾,来保证无线主机与无线接入点 AP 之间的数据帧传输质量。但是802.11 协议并没有对 DRS 算法做具体的规定,而是由无线网络设备生产厂商自行定义。

多数无线网络厂商的 DRS 机制是根据主机无线网卡接收信号的强度、信噪比与帧传输错误率来决定数据速率的调整策略的。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

4-7-5 分析：设计这道习题的目的是帮助读者进一步加深对 802.11 物理层对 2.4GHz 频段信道划分方法的理解。

（1）802.11 标准将 2.4GHz 频段划分为 14 个独立信道。

（2）信道 1 的 fc_1＝2.412GHz，频带宽度为 22MHz，频率范围是 2.401～2.423GHz。两个信道中心频率间隔 5MHz，那么信道 2 的 fc_2＝2.417GHz，频带宽度为 22MHz，频率范围是 2.406～2.428GHz。

（3）相邻信道频率之间会有重叠，即信道 1 和信道 2 之间的频率是有重叠的。为了降低相邻信道由于频率重叠造成的信号干扰，IEEE 选择信道的原则是要相隔五个信道。

（4）按照这个原则，要从以上 14 个信道中选出三个信道，那么只能是 D 中表示的信道 1、6、11。

从以上分析中可以看出，C 的描述是错误的。

答案：C。

4-7-6 分析：在设计无线网络结构时，必须采用信道复用的方法。

Wi-Fi 的信道复用也称为多信道结构。为了避免同频或邻频干扰，图 4-8 给出了一个利用 2.4GHz 的 1、6、11 这三个信道进行复用的蜂窝结构示意图。这种结构与传统的电信移动通信网的蜂窝结构很类似。

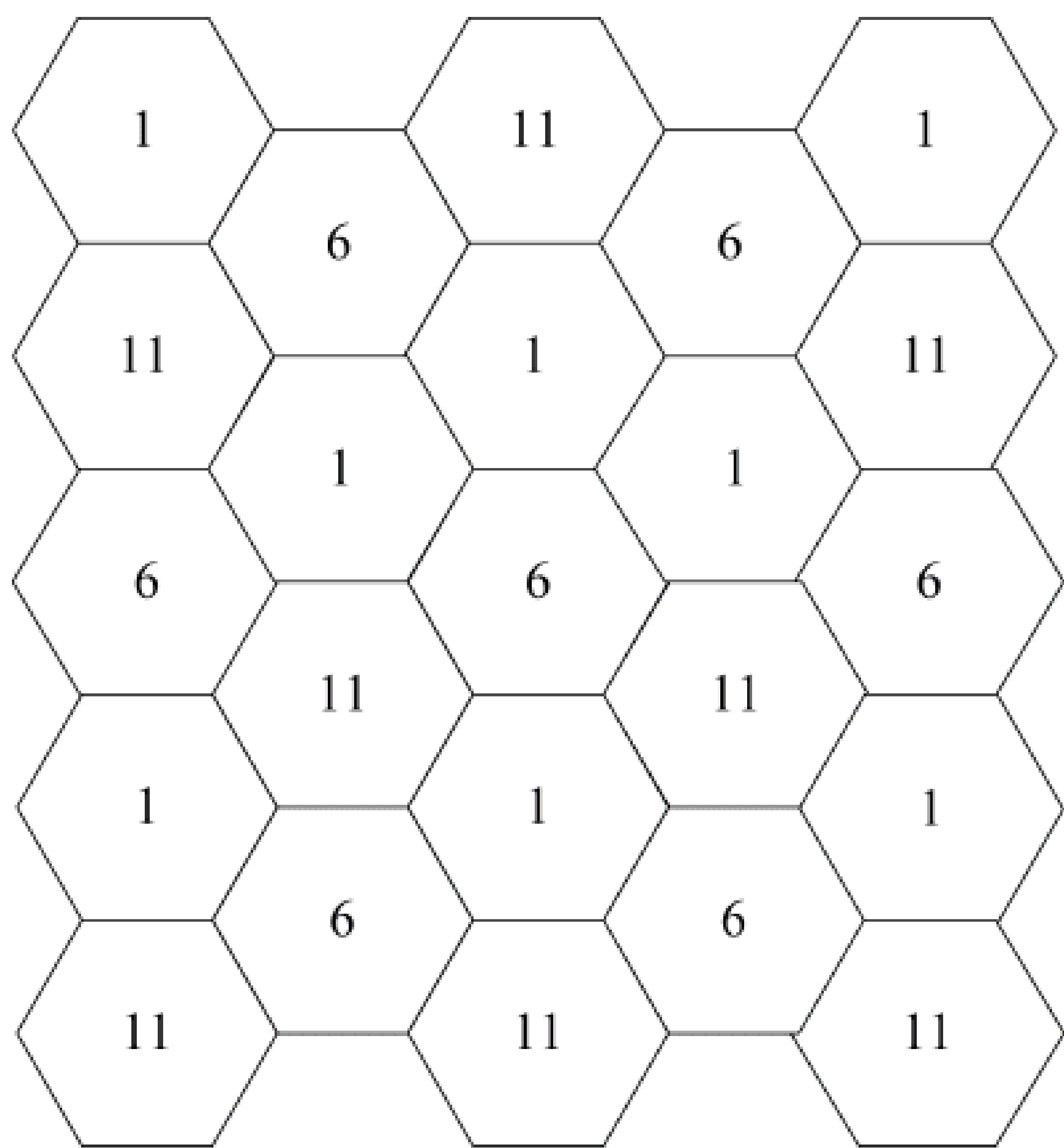


图 4-8 信道频率分布示意图

4-7-7 分析：设计这道习题的目的是帮助读者进一步加深对 802.11 组网特点的理解。

（1）802.11 标准定义了两类组网的结构模式：基础设施模式（infrastructure mode）与独立模式（independent mode）。

（2）基础设施模式也称为“基础结构型”。基础设施模式可以进一步分为基本服务集 BSS 与扩展服务集 ESS。

（3）对应于独立模式的是独立基本服务集（independent BSS）。独立基本服务集主要是

指无线自组网 Ad hoc 网络。

(4) 2011 年的修正案 IEEE 802.11s—2011 又增加了第四种混合模式,对应的是 Mesh 基本服务集(MBSS)。

从以上分析中可以看出,C 的描述是错误的。

答案:C 。

4-7-8 分析:设计这道习题的目的是帮助读者进一步加深对 802.11 的 BSS 特点的理解。

(1) 802.11 标准规定无线局域网的基本构建单元是基本服务集 BSS。BSS 是由一个基站 AP 与若干在逻辑上彼此关联的无线主机组成的。BSS 覆盖的范围叫做基本服务区(BSA)。

(2) BSS 是由接入点 AP 设备与多个无线主机组成。一个 BSS 覆盖范围的一般在几十米到几百米,可以覆盖一个实验室、教室或家庭。

(3) 为了保证无线局域网覆盖用户活动的范围,使所有无线主机可以在 BSA 范围内自由地移动,需要事先对 AP 设备的位置进行勘察、选址与安装。

(4) BSS 中所有主机通过基站 AP 交换数据,形成了一个以基站 AP 为中心节点的星形拓扑构型。

从以上分析中可以看出,B 的描述是错误的。

答案:B。

4-7-9 分析:设计这道习题的目的是帮助读者进一步加深对 802.11 的 ESS 特点的理解。

理解 ESS 结构的基本概念,需要注意几个主要问题:

(1) ESS 中的无线主机 A 可以通过基站 AP1、以太网交换机、基站 AP2 与 ESS 中的任何一台无线主机通信;也可以通过基站 AP1、以太网交换机与路由器接入到主干网,访问 Internet 中的 Web 服务器或主机 N,这样就构成了一个更大的分布式系统(Distribution System,DS)。

(2) 由于 Ethernet 应用非常广泛,因此一般是用以太网去连接多个 BSS,但是也可以通过无线网桥、无线路由器将多个 BSS 连接起来,构成无线分布式系统(Wireless DS,WDS)。在 ESS 结构中,AP 的角色就是一种无线主机访问分布式系统 DS 的接入设备。

(3) 802.11—2007 协议描述帧交互过程,将“无线主机向 AP 发送数据帧”定义为“去往分布式系统(DS)”,将“AP 向无线主机发送的数据帧”定义为“来自分布式系统(DS)”。

(4) 由于 ESS 是由多个 BSS 构成,为了保证主机在 ESS 覆盖范围内无缝漫游,相邻 BSS 覆盖的区域之间必然要有重叠。大部分厂商建议:BSS 覆盖的区域之间的重叠面积至少保持在 15%~20%以上。相邻 BSS 之间信号干扰问题可采用信道复用的方法解决。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

4-7-10 分析:设计这道习题的目的是帮助读者进一步加深对 Ad hoc 网特点的理解。

Ad hoc 网的特点表现在以下几个方面:

第一,自组织与自修复。

Ad hoc 网络可以不需要任何预先架设的无线通信基础设施,所有主机通过分层的协议

体系与分布式路由算法来协调相邻无线主机之间的通信关系。无线主机可以快速、自主和动态地组网。当新的主机接入与退出，或主机之间无线信道出现故障的，无线主机能够寻找新的相邻主机，重新组网。

第二，无中心。

Ad hoc 网络是一种对等结构的无线网络。网络中所有主机的地位平等，没有专门的路由器。任何主机都可以随时加入或离开网络，网络中一台主机出现故障不会影响整个网络系统的工作。

第三，多跳路由。

由于受到主机无线发射功率的限制，每台主机的覆盖范围都有限。在覆盖范围之外的主机之间通信，必须通过中间节点，以多跳转发方式来完成。每台主机同时承担路由器与客户机的功能。

第四，动态拓扑。

由于 Ad hoc 网络允许无线主机根据自己的需要开启或关闭，并且允许主机在任何时间以任意速度和在任何方向上移动，同时受主机的接收信号灵敏度、天线覆盖的范围、主机的地理位置与主机之间障碍物遮挡，以及信号多径传输、信道之间干扰等因素的影响，使得主机之间的通信关系会不断变化，造成了 Ad hoc 网络的拓扑的动态改变。

从以上分析中可看出，C 的描述是错误的。

答案：C。

4-7-11 分析：设计这道习题的目的是帮助读者进一步加深对无线 Mesh 网络特点的理解。

无线 Mesh 网络又叫作“Mesh 基本服务集（MBSS）”或“无线网状网（WMN）”。无线 Mesh 网络的特点可以归纳为以下几点：

(1) 无线 Mesh 网络是由一组呈网状分布的无线 AP 组成，AP 之间通过点对点无线信道连接，形成具有“自组织”“自修复”特点的“多跳”网络。

(2) 从接入的角度，每个无线 AP 都可以形成自己的 BSS；从多跳网络结构角度，AP 又具有接收、转发相邻 AP 发送帧的功能。与传统的 AP 相比，由于无线 Mesh 网络中的 AP 增加了 MAC 层路由选择与自组织的功能，因此无线 Mesh 网络中的 AP 又叫作 Mesh AP。

(3) 无线 Mesh AP 可以形成自己的 BSS，实现主机的接入功能，这一点与 BSS、ESS 相同；从“自组织”与“多跳”的角度，它与 Ad hoc 网络相同，因此，无线 Mesh 网络是混合型网络。

(4) 无线 Mesh 网络与 Ad hoc 网络的区别在于：无线 Mesh 网络是通过 Mesh AP 与 Mesh AP 的点-点连接形成了网状网结构，而 Ad hoc 网络直接由无线主机之间的点-点连接去形成网状网。

(5) 无线 Mesh 网络主要适应于大面积、快速与灵活组网的应用需求；而 Ad hoc 网络主要适用于多主机在移动状态下自主组网的应用需求。

无线 Mesh 网络中的 AP 增加了 MAC 层路由选择与自组织的功能，因此无线 Mesh 网络中的 AP 又叫作 Mesh AP。因此，D 的描述是错误的。

答案：D。

4-7-12 分析：由于无线通信的特殊性，802.11 的 BSS 中也存在着“冲突”现象。理解

这个问题需要注意以下几点：

(1) 当BSS中一台主机向另一台主机发送数据帧时，首先将帧发送到基站AP。

(2) AP是利用共享的无线信道，由AP通过“广播”方式将该数据帧转发出去。

(3) 在基站AP覆盖范围内的所有主机都接收到该帧。只有与该帧目的地址相同的主机能接收并处理该帧，目的地址不匹配的主机丢弃该帧。

(4) 这就出现与传统以太网相类似的“冲突”问题。如果有两个或两个以上无线主机，试图同时利用共享无线信道发送帧时，就会发生“冲突”。

(5) IEEE 802.11的MAC层协议必须解决多个无线主机对共享无线信道的争用问题。

从以上分析中可以看出，AP是通过“广播”方式，而不是“点对点”方式转发数据帧。因此，B的描述是错误的。

答案：B。

4-7-13 分析：理解802.11协议BSS结构的SSID与BSSID定义与特征，需要注意以下几个问题：

(1) 在无线局域网中必须解决AP设备与接入主机的识别问题。802.11协议定义了AP的服务集标识符(SSID)与基本服务集标识符(BSSID)的概念。

(2) 当网络管理员安装AP设备时，首先要为这个AP分配一个服务集标识符SSID与通信信道。AP设备的名字最长为32个字符，并且区分字符的大小写。

(3) 大部分情况下“基本服务集标识符BSSID”就是无线网卡的MAC地址。之所以说是大部分情况下，是因为有的网络设备生产商也允许使用虚拟BSSID。

(4) IEEE 802.11标准规定的无线网卡BSSID与网卡的MAC地址相似，长度都是6字节(48位)。BSSID作为AP设备唯一的标识，在无线主机的漫游中起到了重要的作用。

从以上分析中可以看出，在BSS组网结构中BSSID数值是不能由网络管理员分配。因此，D的描述是错误的。

答案：D。

4-7-14 分析：设计这道习题的目的是帮助读者进一步加深对802.11无争用服务与争用服务特点的理解。

(1) 802.11的MAC层协议支持两种基本的访问控制方式：无争用服务与争用服务。

(2) 在点协调功能(PCF)工作模式中，基站AP控制着多个无线主机对共享无线信道的无冲突访问，形成了以基站为中心的星形网络结构，无争用服务系统的中心是基站——无线接入点AP，因此点协调功能PCF模式提供的是无争用服务。

(3) 802.11的MAC层也可以采用载波侦听多路访问CSMA/CA的介质访问控制方法。人们将802.11协议提供的有争用的服务能力称为“分布协调功能(DCF)”。

(4) 802.11标准规定MAC层都必须支持分布协调功能DCF，而点协调功能PCF是可选的。在默认状态下，802.11的MAC层工作在DCF模式；只有在对传输时间要求高的视频、音频会话类应用中，才会启用点协调功能PCF。

(5) 有些应用需要Wi-Fi提供比“尽力而为”的DCF更高一级的服务，但是又不需要PCF集中控制的服务，人们开始研究混合协调(HCF)的控制方式，但是目前HCF控制方式仍处于研究阶段，并没有相应的协议标准。

从以上分析中可以看出，D的描述是错误的。

答案：D。

4-7-15 分析：设计这道习题的目的是帮助读者进一步加深对传统 Ethernet 局域网与 Wi-Fi 无线局域网在 MAC 方法上的不同之处的认识。

传统 Ethernet 局域网与 Wi-Fi 无线局域网在 MAC 方法上的不同表现在以下几点：

(1) Ethernet 节点在监测到总线空闲时，立即发送帧；而 Wi-Fi 无线局域网节点在检测到无线信道空闲时，不是立即发送帧，而是要求所有准备发送数据帧的主机都执行退避算法，通过冲突避免(CA)来有效地减小冲突发生的概率。

(2) Ethernet 发送节点只要在"冲突窗口"时间内没有检测出冲突，就确定为发送成功，不需要接收节点发送确认帧；而 Wi-Fi 无线局域网发送节点需要等待接收节点发送回的确认帧，来判断此次发送是否成功。这是 Ethernet 与 Wi-Fi 在 MAC 层重要的区别之一。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

4-7-16 分析：设计这道题目的目的是帮助读者理解 802.11 帧间间隔作用。理解 802.11 帧间间隔需要注意以下几点：

(1) 802.11 协议规定所有的无线网卡在检测到信道空闲时真正发送一帧，或者是发送一帧后到发送下一帧时，都需要间隔一段时间，这个时间间隔叫做帧间间隔(Inter Frame Space，IFS)。

(2) 802.11 规定了四种帧间间隔：短帧间间隔 SIFS、点协调功能帧间间隔 PIFS、分布协调功能帧间间隔 DIFS、扩展帧间间隔 EIFS。

(3) 帧间间隔的长短取决于发送帧的类型。高优先级的帧等待的时间短，低优先级的帧等待的时间长。

(4) 802.11 规定的短帧间间隔 SIFS 长度为 28μs。使用到 SIFS 间隔的主要有对信道进行预约的 ACK 帧、CTS 帧，以及属于一次对话的各个帧。

(5) 分布协调功能帧间间隔 DIFS 长度为 128μs。在 DCF 方式中，发送数据帧、管理帧需要用到 DIFS 间隔。

802.11 协议规定：所有的无线网卡在检测到信道空闲时真正发送一帧，或者是发送一帧后到发送下一帧时都需要间隔一段时间。因此，A 的描述是错误的。

答案：A。

4-7-17 分析：设计这道习题的目的是帮助读者加深对几个常用的 MAC 协议特点的认识。

(1) 码分多址 CDMA 是物理层的问题，不属于 MAC 层协议。

(2) CSMA 是一种典型的分布式 MAC 层控制方法，它与 CSMA/CD 都不提供对是否正确接收帧的确认。

(3) CSMA/CA 是无线局域网的 MAC 层控制方法，它提供对接收帧的确认功能。

由于 Ethernet 的 CSMA/CD 方法已经比较普及，因此初学者往往不太注意 CSMA/CA 的这个特点。

答案：D。

4-7-18 分析：在讨论 802.11 发送与接收帧过程时，需要注意以下几点：

(1) CSMA/CA 要求物理层对无线信道进行载波监听。根据接收到的信号强度来判断是否已经有主机利用无线信道发送数据信号。

(2) 当源主机确定信道空闲时,首先要等待一个 DIFS 时间间隔;如果时间到,并且信道仍然空闲则发送第一个帧。

(3) 目的主机在正确地接收到发送帧,并等待 SIFS 时间间隔之后,向发送主机发出 ACK 确认帧。

(4) 帧发送结束后,源主机需要等待接收帧的目的主机发送回的 ACK 确认帧。

源主机在"规定的时间内"接收到 ACK 确认帧,说明没有发生冲突,第一帧发送成功,而不是"任何时间"。因此,D 的描述是错误的。

答案:D。

4-7-19 分析:在讨论 802.11 的 VCS 与 NAV 机制特点时需要注意以下几个问题。

(1) 802.11 的 MAC 层还采用虚拟监听(VCS)与网络分配向量(NAV)机制的目的是:通过主动避免冲突的发生,进一步减小冲突发生的概率。

(2) 802.11 的 MAC 层在帧头的第 2 个字段是"持续时间(Duration/ID)"字段。发送主机在发出一帧时,同时在该字段内填入以 μs 为单位的值,表示在该帧发送结束后,还要占用信道的时间。这个时间包括目的主机返回确认 ACK 帧的时间。

(3) 无线局域网中的其他主机在收到数据帧中"持续时间"的通知后,如果该值大于自己的 NAV 值,根据接收的"持续时间"字段值来修改自己的 NAV 值。

(4) NAV 计时器值随着时间推移递减,只要 NAV 不为 0,主机就认为信道忙,不发送数据帧。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

4-7-20 分析:在讨论 802.11 的 CSMA/CA"冲突退避"概念时,需要注意以下几点:

(1) 由于考虑到可能有多个主机在同一时刻都出现了 NAV=0,都会认为信道空闲,这时多主机同时发送数据帧而出现冲突,因此主机不能立即发送帧。

(2) 802.11 协议规定:所有主机在 NAV 值为 0 之后,需要再等待一个 DIFS 时间。

(3) 在等待一个 DIFS 时间之后,再执行"二进制指数退避算法"。

(4) 这样做的目的是希望能够进一步减少出现冲突的概率。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

4-7-21 分析:在讨论 802.11 的二进制指数退避算法时,需要注意以下几点:

"二进制指数退避算法"规定:

(1) 第 i 次退避时间可以在 2^{2+i} 个时间片[$2^{2+i}-1$]中随机地选择一个。

(2) 第 1 次退避 $i=1$,$2^{2+1}=8$,那么可以在[0,1,…,7]共 8 个时间片中随机地一个退避时间,例如选择 5 个时间片。那么在第一次出现冲突之后,主动延时 5 个时间片。第 2 次退避是 $2^{2+2}=16$ 个时间片,即[0,1,…,15],如果随机选择 12 个时间片,那么在第 2 次出现冲突之后主动延时 12 个时间片。

(3) 802.11 协议将退避时间变量 i 定义为退避变量,退避变量的最大值 $i_{max}=6$。当冲突出现到第 6 次,即 $i=6$ 时,即 $2^{2+6}=256$,可以在[0,1,…,255]的时间片中随机地选择一

个退避时间片。

从以上分析中可以看出，C的描述是错误的。

答案：C。

4-7-22 分析：在讨论802.11的CSMA/CA与802.3的CSMA/CD区别时需要注意以下几点：

(1) 802.3的CSMA/CD要求发送主机在监听到总线空闲时，立即开始发送帧。802.11的CSMA/CA在无线信道从“忙”转到“闲”时，无线网卡不是“立即”发送数据帧，而是要求所有准备发送数据帧的主机等待一个DIFS时间，再执行退避算法。

(2) 802.3协议采用的是“截止二进制指数退避算法”，802.11采用的是“二进制指数退避算法”。算法的计算公式不一样。802.3协议规定一个帧重发的最大次数为16，而802.11协议规定一个帧重发的最大次数为6。

(3) 802.3协议依靠以太网卡的载波侦听，来判断共享总线的忙闲状态。802.11协议设置了虚拟监听VCS与网络分配向量NAV，发送主机通过发布NAV值去向其他主机通知预约无线信道的占用时间，接收主机要根据接收到发送主机的NAV值，随机调整各自的退避时间，进一步减小冲突发生的概率。

(4) 802.3协议不要求目的主机在接收数据帧后发送ACK确认帧，以太网卡在发送一帧的过程中只监测是否出现冲突。如果没有发现冲突，就认为该帧发送成功。MAC协议不保证发送帧被目的主机正确接收。如果该帧在发送过程中没有出现冲突，而是其他传输环节造成帧丢失，这类问题只能靠高层协议去解决。802.11协议要求源主机必须等待目的主机发送回ACK确认帧，才能够判断一帧是否发送成功，因此802.11的MAC协议属于“停止等待协议”。

从以上分析中可以看出，A的描述是错误的。

答案：A。

4-7-23 分析：讨论802.11设备标出的速率值与能够提供给用户的吞吐量问题，需要注意以下问题：

802.11的MAC协议属于“停止等待协议”。停止等待类协议的优点是提高了传输的可靠性，缺点是系统工作效率较低。如果在803.11设备上看到标有300Mbps的字样，往往会认为这台设备能够提供的吞吐量为300Mbps。但是，由于802.11的无线信道在一个时刻只能被一个无线主机占用来发送数据，执行CSMA/CA算法、帧分片、帧加密与解密都会产生额外的带宽开销，使得可以为用户提供的吞吐量不会超过设备标识吞吐量的50%。因此，在供选择的4个速率中，只有D是可能的。

答案：D。

4-7-24 分析：设计这道习题的目的是加深读者对802.11的CSMA/CA控制算法的理解。

(1) 根据题目给出的假设条件，可以做出以下的分析：

① 在802.11b的BSS中，AP只关联了主机A与主机B，以CSMA/CA方式工作。

② 主机A用最长的2342B数据帧向主机B发送数据，AP以长度为14B的ACK帧进行确认。主机B不向主机A发送数据。BSS中不会出现冲突。

③ 不考虑其他控制帧与管理帧的交互，只考虑主机A、B在由AP转发数据帧、ACK帧

的发送延时,AP与主机A、主机B的传输速率相同,设为R(bps)。

(2) 简化后的主机A通过AP转发给主机B的1个数据帧的过程如图4-9所示。

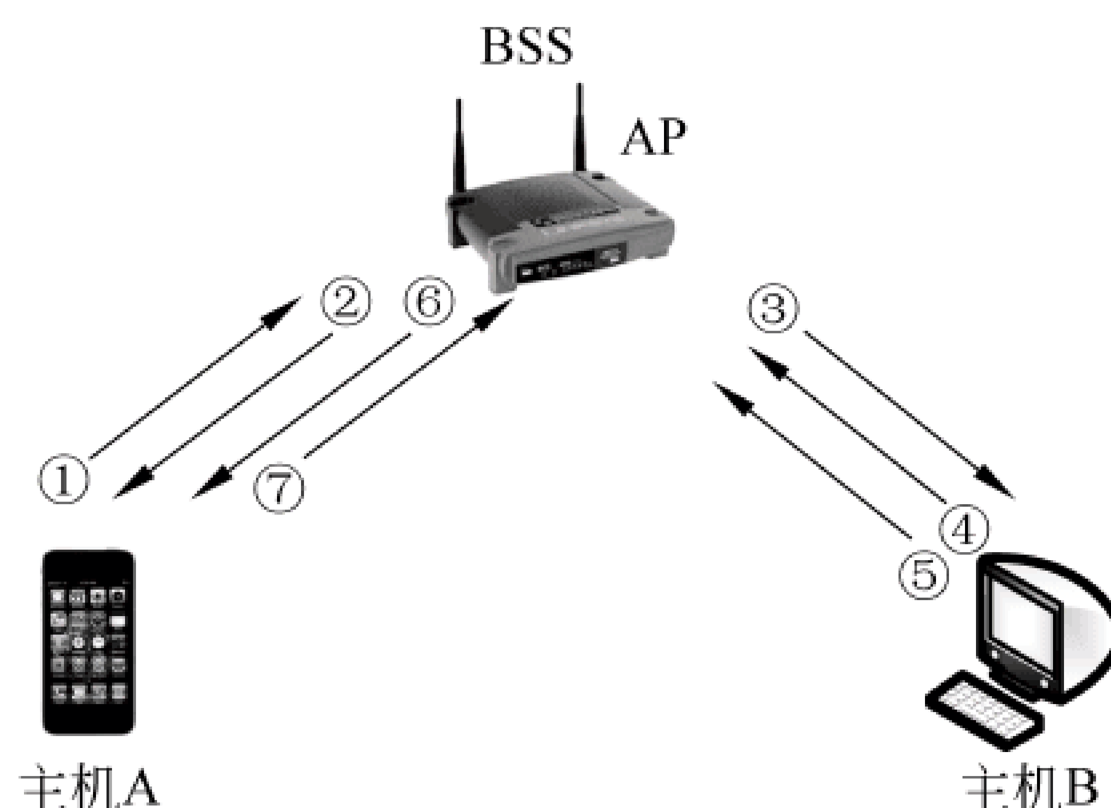


图4-9 AP转发数据帧过程示意图

主机A通过AP转发给主机B的1个数据帧的过程为:

① 主机A将长度为最长的2342B数据帧(帧头长度为30B,帧最大长度为2312B)发送给AP,发送延时$t_1=2342\times8/R$。

② AP向主机A发送长度为14B的ACK确认帧。发送延时$t_2=14\times8/R$。

③ AP向主机B转发送长度为2342B数据帧。发送延时$t_3=2342\times8/R$。

④ 主机B向AP发送长度为14B的ACK确认帧。发送延时$t_4=14\times8/R$。

⑤ 主机B向主机A发送长度为14B的ACK确认帧,用于对数据帧的确认。发送延时$t_5=14\times8/R$。

⑥ AP向主机A转送长度为14B的ACK确认帧。发送延时$t_6=14\times8/R$。

⑦ 主机A向AP发送长度为14B的ACK确认帧。发送延时$t_7=14\times8/R$。

这样,主机A向主机B发送一个数据帧的时间:

$$\begin{aligned}T_0&=t_1+t_2+t_3+t_4+t_5+t_6+t_7\\&=2t_1+5t_2\\&=(2\times2342\times8+5\times14\times8)/R\\&=(37\ 472+560)/R\\&=38032/R\end{aligned}$$

(3) $R=11\text{Mbps}=11\times10^6\text{bps}$

$T_0=38032/11\times10^6=3.457(\text{ms})$

主机A每秒钟发送的数据帧数:

$$N=1/T_0\approx289(\text{帧})$$

主机A的有效数据传输速率:

$$R_{01}=289\times2342\times8\approx5.42\text{Mbps}$$

$$R=11\text{Mbps}=1\times10^6\text{bps}$$

$$T_0=38032/1\times10^6\approx38(\text{ms})$$

主机A每秒钟发送的数据帧数:

$$N=1/T_0\approx26(\text{帧})$$

主机A的有效数据传输速率:

$$R_{02}=26\times2342\times8\approx0.5\text{Mbps}$$

答案:

(1) 传输速率为11Mbps时,主机A每秒钟发送的数据帧数约为289帧,有效数据传输速率约为5.42Mbps。

(2) 传输速率为1Mbps时,主机A每秒钟发送的数据帧数约为26帧,有效数据传输速

率约为0.5Mbps。

4-7-25 分析：

(1) 信标帧是无线局域网的“心跳(Beacon)”。在BSS模式中，AP以0.1～0.01s的时间间隔周期性地广播信标(Beacon)帧。

(2) 信标帧在无线主机与AP关联过程中的作用主要表现在以下三个方面：

- 无线主机从接收到的信标帧可以发现可用的基站AP。
- 信标帧为无线主机接入到AP提供了必要的配置信息。
- 无线主机从接收信标帧时间戳中提取AP的时钟，使无线主机与AP保持时钟同步。

(3) 在BSS模式中，AP发送信标帧；只有在Ad hoc模式中，无线主机发送信标帧。

(4) 802.11协议允许AP管理员通过设置，改变信标帧广播周期，但是不能禁用信标帧。

从以上分析中可以看出，A的描述是错误的。

答案：A。

4-7-26 分析：

(1) 无线主机在接入AP之前，可以通过被动扫描或主动扫描的方式来发现AP。

(2) 无线主机扫描信道与监听信标帧的过程称为被动扫描。在被动扫描状态下，如果有多个AP向主机发送了信标帧。主机选择其中一个，并向AP发送了关联请求帧；主机AP向主机发送了关联应答帧。

(3) 无线主机也能通过向位于无线主机覆盖范围内的所有AP广播探测帧，来实现主动扫描。在主动扫描状态下，主机广播信标帧。接收到信标帧的多个AP都给主机发送探测响应帧。主机选择其中一个AP，向AP发送了关联请求帧。AP向主机返回了关联应答帧。

从以上分析中可以看出，D的描述是错误的。

答案：D。

4-7-27 分析：

(1) 802.11协议支持两种级别的链路认证：开放系统认证与共享密钥认证。

(2) 开放系统认证是默认的。无线主机与AP交换一次“链路认证请求帧”与“链路认证应答帧”。无线主机将自己的MAC地址通报给AP。AP与无线主机之间不进行任何的身份信息识别，所有请求主机的无线网卡都可以通过认证。

(3) 只有在Wi-Fi Free的公开、免费使用状态下，才使用开放系统认证。如果用户对主机的无线网卡有任何控制需求，都不能使用开放系统认证。

(4) 共享密钥认证采用的是有线等效协议(WEP)或无线保护访问(WPA)协议。实践证明，WEP协议的安全性较差，IEEE 802.11i工作组用安全性高的WAP协议取代了WEP协议。

从以上分析中可以看出，D的描述是错误的。

答案：D。

4-7-28 分析：设计这道习题的目的是帮助读者进一步加深对802.11无线主机与AP关联关系的理解。

(1) 关联只能是由无线主机发起，并且一个时刻一台无线主机只能与一个AP关联。

关联属于一种记录保持的过程,它帮助分布式系统记录每台无线主机的位置信息,保证将帧传送到目的主机。当无线主机从原AP覆盖的范围移动到新的AP覆盖的范围,需要执行“重关联”的过程。

(2) AP与无线主机都可以通过发送解除关联帧,断开当前关联的AP。无线主机离开无线网络时应该主动执行解除关联的操作。如果AP发现关联的无线主机信号消失,AP将采取超时机制来解除与该无线主机的关联。

从以上分析中可以看出,A的描述是错误的。

答案:A。

4-7-29 分析:讨论802.11的AP接受主机关联的问题,需要注意以下几点:

(1) 802.11协议并没有对主机选择AP进行关联的条件进行规范,而是由生产AP设备的厂商决定。比较常用的方法是考虑两个主要的因素。

① AP从“关联请求帧”了解无线主机是否具有以基本传输速率通信的能力。

例如,AP可以要求无线主机必须能够以1Mbps、2Mbps基本的低传输速率通信,也可以用较高的4.5Mbps与11Mbps传输速率。

② AP能否为申请关联的无线主机提供所需的缓冲空间。

因为当一个主机关联上一个AP时,主机会向AP通告它选择了一直可以接收和发送数据的主动模式,还是选择节能模式。当选择节能模式的主机处于休眠状态时,所有发往这个主机的数据帧都要先缓存在AP上。

(2) 聆听间隔(listen interval)是AP为关联的无线主机缓冲数据的最短时间。AP在关联时需要根据“关联请求帧”中的“聆听间隔”时间长短,来预测无线主机需要的缓冲空间大小。如果AP能够提供足够的缓存空间,则接收;如果不能提供足够的缓存空间,则拒绝。

(3) 如果满足以上基本条件,则同意与该无线主机建立关联,AP回送一个“关联应答帧”。

从以上分析中可以看出,A的描述是错误的。

答案:A。

4-7-30 分析:理解Wi-Fi中“漫游”与“重关联”的过程,需要注意以下几个问题:

(1) 漫游(roaming)是指:无线主机在不中断通信的前提下,在不同AP覆盖范围之间移动的过程。802.11标准中并没有用到漫游这个术语。人们对这种现象的解释是:不论何时何地,是否漫游都是客户端的自由。

(2) 漫游的决定权由无线主机用户掌握,802.11协议并没有对主机在什么情况下要启动漫游做出明确的规定。无线主机是否漫游的规则是由无线网卡制造商制定的。无线网卡一般是根据信号的质量来决定是否要启动漫游和重关联的过程。这里的信号质量主要是指信号强度、信噪比与信号传输的误码率。

(3) 从MAC层看,漫游就是无线主机转换AP的过程。从网络层及以上高层看,漫游就是在转换接入点的同时仍然维持原有网络连接的过程。从一个AP漫游到另一个信道AP的过程只涉及第二层的MAC地址的寻址问题,因此它又叫作“二层漫游”。跨网络(涉及IP地址寻址)的无线主机漫游叫作“三层漫游”。

(4) 无线网卡在通信过程中会每隔几秒就在其他信道上发送探询帧。通过持续的主动扫描,无线主机可以维护和更新已知的AP列表,以便在无线主机在漫游时使用。无线主机

可以与多个 AP 认证，但是只和一个 AP 关联。

(5) 由于 ESS 中的原 AP 与新 AP 通过连接它们的分布式系统 DS 交换了漫游主机的信息，因此不需要发送“解除关联帧”。

从以上分析中可以看出，A 的描述是错误的。

答案：A。

4-7-31 分析：理解 RTS/CTS 预约模式工作过程，需要注意以下几个问题：

(1) 源主机在检测到信道空闲，并退避一个 DIFS 时间之后，发生一个短的“请求发送(RTS)帧”。RTS 帧包括源主机地址、目的主机地址以及这次通信需要占用的持续时间。

(2) 当目的主机接收到 RTS 帧，并且信道空闲，再退避一个 SIFS 帧间隔时间后，发送一个短的“允许发送(CTS)帧”。CTS 帧复制 RTS 帧中“这次通信需要占用的持续时间”的数值。源主机之外的其他主机在接收到 CTS 帧之后，将根据 RTS 帧中“这次通信需要占用的持续时间”的数值来设置本主机的 NAV 值。

(3) 源主机在接收到 CTS 帧，退避 SIFS 帧间隔时间后，发送数据帧。

(4) 目的主机在接收到数据帧之后，退避 SIFS 帧间隔后，向源主机发送 ACK 确认帧。

(5) RTS/CTS 对信道的预约可以有效地解决隐藏主机带来的冲突问题。

从以上分析中可以看出，B 的描述是错误的。

答案：B。

4-7-32 分析：了解 802.11 数据帧结构，需要注意以下几点：

(1) IEEE 802.11 数据帧是由帧头、数据字段与帧尾 3 部分组成的。

(2) 帧头长度为 30B，数据字段长度在 0～2312B，帧尾是由 2B 的帧校验字段组成。

(3) 帧头是由帧控制、持续时间、地址 1～地址 4 与序号 7 个部分组成的。

与 802.3 协议相比，802.11 帧中地址字段比较复杂，需要引起读者的注意。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

4-7-33 分析：设计这道练习题的目的是加深读者对 802.11 数据帧控制字段含义与作用的理解。数据帧中的第一个字段是帧控制字段。控制字段最为复杂。2 个字节长的帧控制字段包括 11 个子字段。类型与子类型的长度与含义是：

(1) 类型——2bit，表示不同类型的帧。其中：

① 00 表示管理帧。

② 01 表示控制帧。

③ 10 表示数据帧。

(2) 子类型——4bit，表示不同类型帧的子类型。

在管理帧中：

① 0000 表示关联请求帧。

② 0001 表示关联响应帧。

③ 0100 表示探询请求帧。

④ 0101 表示探询应答帧。

⑤ 1000 表示信标帧。

在控制帧中：

① 1011 表示 RTS 帧。

② 1100 表示 CTS 帧。

③ 1101 表示 ACK 帧。

在数据帧中：

① 0000 表示数据帧。

② 0100 表示无数据的空帧。

③ 1000 表示 QoS 数据帧。

如果类型与子类型的 6 个比特为 00 0100，表示的是管理帧中的探询请求帧；01 1101 表示的是管理帧中的 ACK 确认帧；00 1000 表示的是管理帧中的信标帧；10 0000 表示的是数据帧。

从以上分析中可以看出，A 的描述是错误的。

答案：A。

4-7-34 分析：802.11 帧控制字段中的电源管理位对移动互联网与物联网的移动终端设备的设计十分有用，需要引起读者的注意。

(1) 电源管理：由于接入无线网络中有大量的设备是笔记本计算机、智能手机与各种手持移动终端，因此节能非常重要，它关系到终端的移动性与续航能力。802.11 协议在帧控制字段中设置了 1 位的“电源管理”位。

(2) 802.11 支持两种电源管理模式：主动模式(Active Mode)与节电模式(Power Save Mode)。

(3) 802.11 协议默认的是主动模式。主动模式表示网卡处于时刻准备发送或接收数据的状态。节能模式是可选的模式。

(4) 在节能模式中，主机关闭无线发射与接收电路，处于“休眠”状态。协议规定：电源管理位为 0，表示源主机在发送完这一帧后仍然处于工作状态；电源管理位为 1，表示源主机在发送完这一帧后进入休眠状态。由于处于主动模式的数据传输速率高于节能模式，而办公室的无线主机由于一直可以连接 220V 电源，因此一般都处于默认的主动模式状态。但是，很多移动终端设备是由内部电池供电，为了延长设备使用时间，可以选择为节能模式。

从以上分析中可以看出，电源管理位为 1，表示源主机在发送完这一帧后进入休眠状态。“休眠”主机要关闭的是无线发射与接收电路，而不是整个节点。因此，B 的描述是错误的。

答案：B。

4-7-35 分析：IEEE 802.11 数据帧最特殊的地方是帧头有 4 个地址字段。

理解 802.11 帧中多个地址字段，需要注意几个问题：

(1) 尽管协议规定帧头有 4 个地址字段，但是这 4 个地址字段并不是都出现在所有的帧中。其中，地址 4 只用于无线自组网 Ad hoc 中。

(2) 在一个 BSS 中，当数据帧从源主机经过 AP 转发到目的主机时，将使用 3 个 MAC 地址：源地址、目的地址与 AP 地址。

按照 IEEE 802.11 数据帧的规定：

① 当源主机向 AP 发送数据帧时，帧控制字段的“去往 DS=1、来自 DS=0”；地址 1=AP 地址，地址 2=源地址，地址 3=目的地址。

② 当 AP 向源主机发送数据帧时，帧控制字段的“去往 DS=0、来自 DS=1”；地址 1=目的地址，地址 2=AP 地址，地址 3=源地址。

从以上分析中可以看出，C 的描述是错误的。

答案：C。

4-7-36 分析：设计这道习题的目的是帮助读者进一步加深对 802.11 无线网卡 MAC 控制器功能的理解。

(1) 802.11 无线网卡的设计方法、基本结构与 Ethernet 网卡是相同的，它覆盖了 MAC 层与物理层的主要功能。802.11 无线网卡同样也由 3 部分组成：网卡与无线信道的接口、MAC 控制器以及网卡与主机的接口。

(2) MAC 控制器是无线网卡的核心，它负责将接收到的主机数据封装成帧，同时根据 CSMA/CA 算法，确定帧什么时候通过基带处理器、数字模拟转换器 DAC，将计算机产生的数字信号转化成适合无线信道发送的信号，然后再通过无线发射器、天线发送出去。802.11 除了要发送和接收主机需要的数据帧之外，还有 802.11 协议自身需要的控制帧与管理帧。MAC 控制器芯片还设置了实时功能模块，自动生成和处理各种 802.11 协议的控制与管理帧。

(3) 大多数无线网卡采用 Card Bus 接口标准，也有些采用 Mini-PCI 接口标准。

(4) 由于无线网卡有可能需要同时处理多个数据帧，因此，网卡可以通过设置 RAM 缓冲区来存储正在处理的数据帧。

(5) 为了快速实现无线通信中的安全功能，MAC 控制器中设置了安全处理单元与密钥缓冲器，以及存储不断更新的加密算法与加密程序的闪存(Flash Memory)。

(6) 802.11 无线网卡能够独立于主机操作系统，自主地完成 802.11 协议规定的 MAC 层、物理层与无线通信安全等功能。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

4-7-37 分析：了解 802.11 无线网卡分类，需要注意以下几点：

无线网卡的分类主要有两种方法：一是按网卡支持的协议标准，另一种是按照网卡的接口类型。

(1) 按照无线局域网协议标准进行分类，无线网卡可以分为 802.11b、802.11a、802.11g 与 802.11n 等几种基本类型。

(2) 按照接口类型进行分类，无线网卡可以分为外置无线网卡、内置无线网卡与内嵌无线网卡 3 种主要类型。

(3) 外置无线网卡可以进一步分为 PCI 网卡、PAMCIA 与 USB 网卡。

(4) 笔记本计算机内置的无线网卡主要有 Mini-PCI 与 Mini-PCI Express。

(5) 随着智能手机、PAD、RFID 读写器、智能眼镜等可穿戴技术设备、洗衣机与电冰箱等智能家居、智能机器人大量使用 802.11 技术，推动了支持 802.11 标准的片上系统 SoC 的研究与芯片的问世，促进了内嵌无线网卡的发展。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

4-7-38 分析：了解无线接入点 AP 设备的发展，需要注意以下几个问题。

(1) 第一代无线接入点AP相当于以太网集线器。AP设备通过无线信道与一组无线主机关联,作为BSS的中心节点执行CSMA/CA的MAC算法,实现无线主机之间通信的功能。

(2) 第二代无线接入点AP将无线接入与无线局域网管理功能结合到以太网交换机中,构成了ESS无线网络。

(3) 第三代无线接入点AP与无线局域网控制器结合,可构建更大规模、集中管理的统一无线网络系统。

(4) 无线接入点也可以作为无线网桥,通过无线信道在MAC层实现两个或两个以上的无线局域网,或无线局域网与有线以太网的无线桥接与中继的功能。

(5) 为了方便地接入更多的PC与手机,人们可以利用一台接入以太网的主机下载一种应用软件,将内置或外置的一块无线网卡改造成一个虚拟AP,为其他无线主机或无线终端设备提供接入服务。

(6) 无线接入点AP只能处理MAC地址,无线路由器可以处理IP地址,实现接入Internet的路由功能,因此两者分别属于链路层与网络层的网络设备。在市场上,两者经常不加区别地都叫做无线路由器。

从以上分析中可以看出,D的描述是错误的。

答案:D。

4-7-39 分析:理解802.11“双频多模”AP的研究与应用,需要注意以下几点:

(1) 802.11a、802.11b与802.11g等物理层标准的不同,导致了不同标准的无线设备之间存在着兼容性问题。802.11a工作在5GHz,而802.11b、802.11g工作在2.4GHz;802.11a与802.11b发送信号所采用的调制方式也不相同。

(2) 一台无线主机漫游到不同物理层标准的BSS区域时就必须使用不同的无线网卡,这显然是不合适的。为了解决这个问题,无线AP设备研制向着双频多模(dual band and multimode)方向发展。

(3) “双频”是指可以支持2.4GHz与5GHz两种频率;“多模”是指可以自动识别和支持802.11a、802.11b与802.11g等多种物理层标准。

从以上分析中可以看出,D的描述是错误的。

答案:D。

4-7-40 分析:了解802.11动态VLAN的概念,需要注意以下几点:

(1) 第一代AP只是将所有接入的无线主机连接到同一无线局域网中,不能为不同用户提供区分服务。“动态VLAN”是将以太局域网中的虚拟局域网技术引入到Wi-Fi中,结合无线局域网的身份认证机制,实现在一个BSS中为有不同需求的用户提供区分服务的功能。

(2) 802.1x协议是在MAC层实现基于Client/Server的访问控制和认证协议。无线主机访问AP之前,需要按照802.1x的规定进行的用户/设备的认证。

(3) 无线主机接入到AP之前首先向身份认证服务器(Radius Server)发出认证请求。身份认证服务器通过对无线主机的身份认证之后,向AP与主机发回的“access accept”帧,为无线主机指定某个VLAN。不同VLAN的无线主机经过身份认证之后,将被分配到不同的VLAN中。

(4) 属于同一 VLAN 的无线主机都会获得相同的密钥。无线主机发送的数据帧到达 AP 时,AP 会自动转发到它所属的 VLAN。

从以上分析中可以看出,C 的描述是错误的。

答案:C。

4-7-41 分析:理解 802.11 统一无线网络的概念,需要注意以下几个问题:

(1) 随着 Wi-Fi 从初期的家庭、小型办公室环境的应用扩大到覆盖一家一个校园、一家大型医院、一个科技园区,从几个 AP 设备扩展为由数百个 AP 设备的大型无线网络系统,促使 Wi-Fi 网络结构从初期以自主 AP 为中心的基本服务集 BSS,发展到用以太网交换机将多个 BSS 互联起来构成的扩展服务集 ESS,直到将以太网交换机变换为无线局域网控制器 WLC,出现了集中管理的大型无线网络结构。

(2) 推动 Wi-Fi 结构由自治方式到集中方式转型的动力主要来自大型无线网络运行、维护与网络管理的压力。集中式管理的统一无线网络的特点,主要表现在以下几个方面:

① 大型的 ESS 系统中 AP 参数配置的困难。

② AP 版本升级、软件缺陷修补与添加新的功能的困难。

③ 大型的无线网络 AP 位置与配置、运维的困难。

(3) 为了解决这些问题,统一无线网络增加了"无线资源管理 RRM"功能。RRM 又称为 Auto-RF。无线资源管理通过连续地采集和监测来自多个 AP 无线信道的数据,利用无线资源管理算法,分析无线通信系统的状态,通过协调多个 AP 的信道频率与功率设置,来提高信号传输质量,增强对无缝漫游的支持能力。Auto-RF 可以降低无线网络系统的维护难度,提高无线网络运行的可靠性与可用性。

(4) 出现统一无线网络 UWN 概念之后,人们将不使用无线局域网控制器 WLC 的 AP 称为"自治"或"基于 IOS 的 AP"。

所谓"自治",是指传统的无线接入点 AP 的操作系统与配置文件存储在设备的存储器中,可以作为一个完整的系统独立工作。

① 自治 AP 系统的功能是通过两类进程(实时进程与管理进程)来实现的。

② 实时进程包括无线信号的发送与接收、MAC 协议工作过程的控制与管理、加密。

③ 管理进程包括无线信道频率与发射功率的管理、关联与漫游的管理、客户端认证、安全与 QoS 管理。

(5) 在统一无线网络中,WLC 使用无线接入点控制与配置(CAPWAP)协议,对大量 AP 的管理进程实现了集中管理,因此人们将统一无线网络中的 AP 称为"瘦 AP"或"轻量级接入点 LAP",将自治 AP 称为"胖 AP"或"分离 MAC 架构"。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

4-7-42 分析:了解 802.11 无线局域网控制器 WLC 功能时,需要注意以下几个问题:

(1) 动态分配信道,优化发射功率。

在由一个 WLC 管理的多个 LAP 结构中,WLC 可以为每个 LAP 选择并配置无线信道频率与发射功率。当某个 LAP 出现故障时,WLC 将自动调高周围 LAP 的发射功率。在有多个 WLC 组成的大型无线网络中,按照 802.11a/b/g/n 的不同信道,WLC 动态地形成多个无线组。每个无线组要"选举"出一个"组长"。无线组以一定的时间间隔(通常是 600s),

由担任组长的WLC向组成员发送信标帧,组成员的通过应答帧,向组长报告信道频率、发射功率、干扰、噪声、接收到的LAP信号功率以及恶意LAP信号等信息。组长WLC根据远程采集到的信息,使用无线资源管理RRM算法来制定无线信道与发射功率的调整方案。WLC通过动态地调整LAP的信道频率与发射功率的方法,达到提高无线通信质量,增强无线网络的可用性与可靠性的目的。

(2) 支持移动主机的二层和三层漫游。

由于WLC以集中方式管理多个LAP,并且建立与各个LAP关联的移动主机用户列表,因此可以方便地实现一个WLC管理的多个LAP关联客户的漫游。在大型的无线网络中,移动主机可以在一个IP子网中的多个WLC之间实现二层漫游,可以在多个IP子网的WLC之间实现三层漫游,整个漫游过程对于移动主机是透明的。

(3) 动态地均衡客户端的负载。

CAPWAP协议支持动态冗余和负荷均衡。LAP在向所有WLC发送CAPWAP发现请求时,WLC返回的发现请求响应帧中包含当前已经接入的LAP数、能够承受最多接入的LAP数量,以及已经关联的用户数。LAP将尝试与最空闲的WLC建立关联,以均衡负荷。在LAP已经与一个WLC建立关联之后,它将周期性地(默认值为30s)发送CAPWAP信标帧,WLC采用单播方式发送响应帧。如果LAP丢失了1个响应帧,它将以1s为间隔连续发送5个信标帧,如果5s之内没有收到响应帧,则说明原WLC"忙"。LAP则重新启动WLC发现过程。

(4) 有效的安全性管理。

每台设备在出厂前预安装了一个X.509证书,LAP和WLC使用数字证书来完成双方的认证,以防止假冒的LAP与WLC侵入统一无线网络中,提高系统的安全性。

从以上分析中可以看出,A的描述是错误的。

答案:A。

第三部分 综合练习——术语解析

从给出的26个定义中挑出20个,并将标识定义的字母填在对应术语前的空格位置。

(1) ________ PCF　　(2) ________ 4B/5B编码

(3) ________ 网桥　　(4) ________ WEP

(5) ________ VLAN　　(6) ________ Ad hoc

(7) ________ STP　　(8) ________ 无线局域网阵列

(9) ________ 共享介质　　(10) ________ 信标帧

(11) ________ WLC　　(12) ________ BSS

(13) ________ 802.11n　　(14) ________ DIFS

(15) ________ 冲突　　(16) ________ 截止二进制指数后退延迟算法

(17) ________ BSSID　　(18) ________ 局域网交换机

(19) ________ VCS　　(20) ________ 冲突窗口

A. 由一个基站AP与若干在逻辑上彼此关联的无线主机组成的网络。

B. 多个主机通过总线发送和接收数据的传输介质。

C. 同一时刻有两个或两个以上主机在一条总线上发送数据出现的问题。
D. 速率最高可达600Mbps的802.11标准。
E. 可在多个端口之间同时建立多个并发连接的局域网设备。
F. Wi-Fi网卡的地址。
G. 定义CSMA/CD总线介质访问控制子层与物理层的标准。
H. 由基站AP控制着多个无线主机对共享无线信道的无冲突访问的工作模式。
I. 分布协调功能帧间间隔。
J. 自组织、无中心、多跳路由与动态拓扑的无线网络。
K. Ethernet网络传播延迟两倍的值。
L. CSMA/CD的后退延迟算法。
M. 虚拟监听机制。
N. Ethernet主机不发送数据帧时应处的状态。
O. 连接在一个缆段上所有节点都能够检测到冲突发生的最短时间。
P. 在共享传输介质或信道上同时出现两个或两个以上帧数据信号的现象。
Q. 交换机只要接收并检测到目的地址字段,不进行差错校验立即转发的方法。
R. 100BASE-T传输比特流采用的信号编码方法。
S. 可通过软件设置的方法将计算机按组织结构划分成多个逻辑工作组的局域网。
T. 将无线局域网控制器WLC与多个接入点AP集成在一个硬件设备。
U. 连接中继器多个缆段的物理层连网设备。
V. 802.11采用的共享密钥认证协议。
W. 在MAC层互联两个或两个以上局域网的设备。
X. 能够自动控制局域网系统的拓扑形成无环路逻辑结构的协议。
Y. 以集中方式管理大型Wi-Fi无线网络系统的网络设备。
Z. 为无线主机接入到AP提供了必要的配置信息。

参考答案:

(1) H	(2) R	(3) W	(4) V	(5) S
(6) J	(7) X	(8) T	(9) B	(10) Z
(11) Y	(12) A	(13) D	(14) I	(15) P
(16) L	(17) F	(18) E	(19) M	(20) O

第 5 章 网络层

第一部分 同步练习

5.1 网络层与 IP 协议

5-1-1 以下关于网络层基本概念的描述中,错误的是________。

A. 网络层要实现路由选择、拥塞控制与网络互联

B. 网络层服务要依赖于通信子网所采用的技术

C. 网络层向传输层端-端传输连接提供服务

D. 网络层具有跨局域网、城域网与广域网的互联网络寻址能力

5-1-2 以下关于异构网络互联的描述中,错误的是________。

A. 异构性是指网络和通信协议、计算机硬件或操作系统上

B. 网络互联异构性主要表现之一是广域网、城域网、局域网的互联

C. 利用路由器将两个或两个以上网络互连起来构成的系统叫作互联网络

D. 利用集线器实现多层级联方法组建的大型局域网系统也是一种互联网络

5.2 IPv4 协议的基本内容

5-2-1 以下关于 IP 协议特点的描述中,错误的是________。

A. IP 协议是点对点的网络层通信协议

B. IP 协议提供的是一种“尽力而为”的服务

C. 无连接并不意味着 IP 协议不维护 IP 分组发送后的状态信息

D. 不可靠意味着 IP 协议不能保证每个 IP 分组都能够正确的到达目的节点

5-2-2 以下关于 IP 分组结构的描述中,错误的是________。

A. IPv4 分组头的长度是可变的

B. 分组头长度最小为 20B,最大为 60B

C. 协议字段表示 IP 协议版本号,值为 4 表示 IPv4

D. 生存时间字段表示一个分组一次传输过程中可以经过的最多的跳数

5-2-3 如果一个路由器接收到一个 IP 分组的前 8 位是 01000010,路由器丢弃了该分组,为什么?

5-2-4 一个分组报头中报头长度(HLEN)字段值为 5_{16}(十六进制),而总长度字段值为 0028_{16}。请问:该分组携带了多少个字节的数据?

5-2-5 以下关于 IPv4 分组校验和的描述中,错误的是________。

A. IPv4 头校验和字段长度为 8 位

B. 校验和对 IP 分组头与分组数据进行的计算

C. IP 分组头的头校验和是为了保证分组头传输安全性

D. IP 分组头中只有 TTL 值每经过一个路由器都一定会变化

5-2-6 以下关于 IP 分组分片基本方法的描述中,错误的是________。

A. 片偏移值是以 8 字节为单位来计数的

B. IP 分组长度大于 MTU 时,就对 IP 分组进行分片

C. 分片 MF 值为 1 表示接收的分片不是最后的一个分片

D. DF=1,分组的长度又超过 MTU,则丢弃该分组,不需要向源主机报告

5-2-7 如果到达的分组的 M 位是 1,分片的偏移值为 0。这是第一个分片,还是最后一个分片,或者是中间的分片?

5-2-8 假设一个 IP 分组头部长度为 20B,数据字段长度为 2000B。分组从源主机到目的主机要经过两个网络。这两个网络允许的最大传输单元分别为 1500B 与 576B。请问:该 IP 分组通过两个网络时需要如何进行分片?

5-2-9 在 IPv4 网络中,路由器转发 IP 分组时分组头的字段值变不变?如果变,哪个(或哪些)字段值在变?为什么?

5-2-10 IPv4 分组的最大长度是________。

A. 65535B　　B. 536B　　C. 1500B　　D. 可变

5-2-11 以下关于 IP 分组头选项特点的描述中,错误的是________。

A. 源路由是由发送分组的源主机制定的传输路径

B. 源路由主要用于测试某个网络的吞吐量,绕开出错网络

C. 严格源路由规定分组要经过的路径上每个路由器,顺序可以改变

D. 松散源路由规定的不是一条完整的传输路径,中间可以经过其他路由器

5-2-12 以下关于 IP 分组头选项时间戳特点的描述中,错误的是________。

A. 时间戳参数可以利用它追踪路由器的运行状态

B. 时间戳记录分组从源路由器发出的时间

C. 时间戳采用的是格林尼治时间

D. 时间戳的单位是毫秒

5-2-13 用二进制方法计算下图所示的 IP 分组头部校验和。

<table>
<tr><td>4</td><td>5</td><td>0</td><td colspan="2">28</td></tr>
<tr><td colspan="3">1</td><td>0</td><td>0</td></tr>
<tr><td colspan="2">4</td><td>17</td><td colspan="2">0</td></tr>
<tr><td colspan="5">10.12.14.5</td></tr>
<tr><td colspan="5">12.6.7.9</td></tr>
</table>

5.3 IPv4 地址

5-3-1 将二进制数 1101111 转换成十进制。

5-3-2 将二进制数 11011110111000000000111101010101 转换成点分十六进制数。

5-3-3 将十六进制 ABACAB32 转换为二进制数。

5-3-4 将十进制数 157 转换为二进制数。

5-3-5 试将二进制 IP 地址"10000001 00001011 00000111 11101111"转换为点分十进制。

5-3-6 试将点分十进制 IP 地址 224.155.25.255 转换为二进制。

5-3-7 A 类、B 类、C 类地址的地址数分别占全部 IP 地址总数的多少?

5-3-8 判断以下每个用二进制数表示的 IP 地址的类型。

A. 00000001 00001101 00001100 0010000

B. 11010000 10000011 00000011 10000011

C. 10100011 10101111 10001110 00011111

D. 11110000 10010011 11011001 00001111

5-3-9 判断以下每个用点分十进制数表示的 IP 地址的类型。

A. 228.12.33.0　　B. 193.1.222.255

C. 12.1.1.1　　D. 134.2.220.255

5-3-10 给出以下每个标准分类 IP 地址的地址掩码与网络地址。

A. 25.1.1.1　　B. 151.1.222.25

C. 193.2.220.250　　D. 222.12.33.1

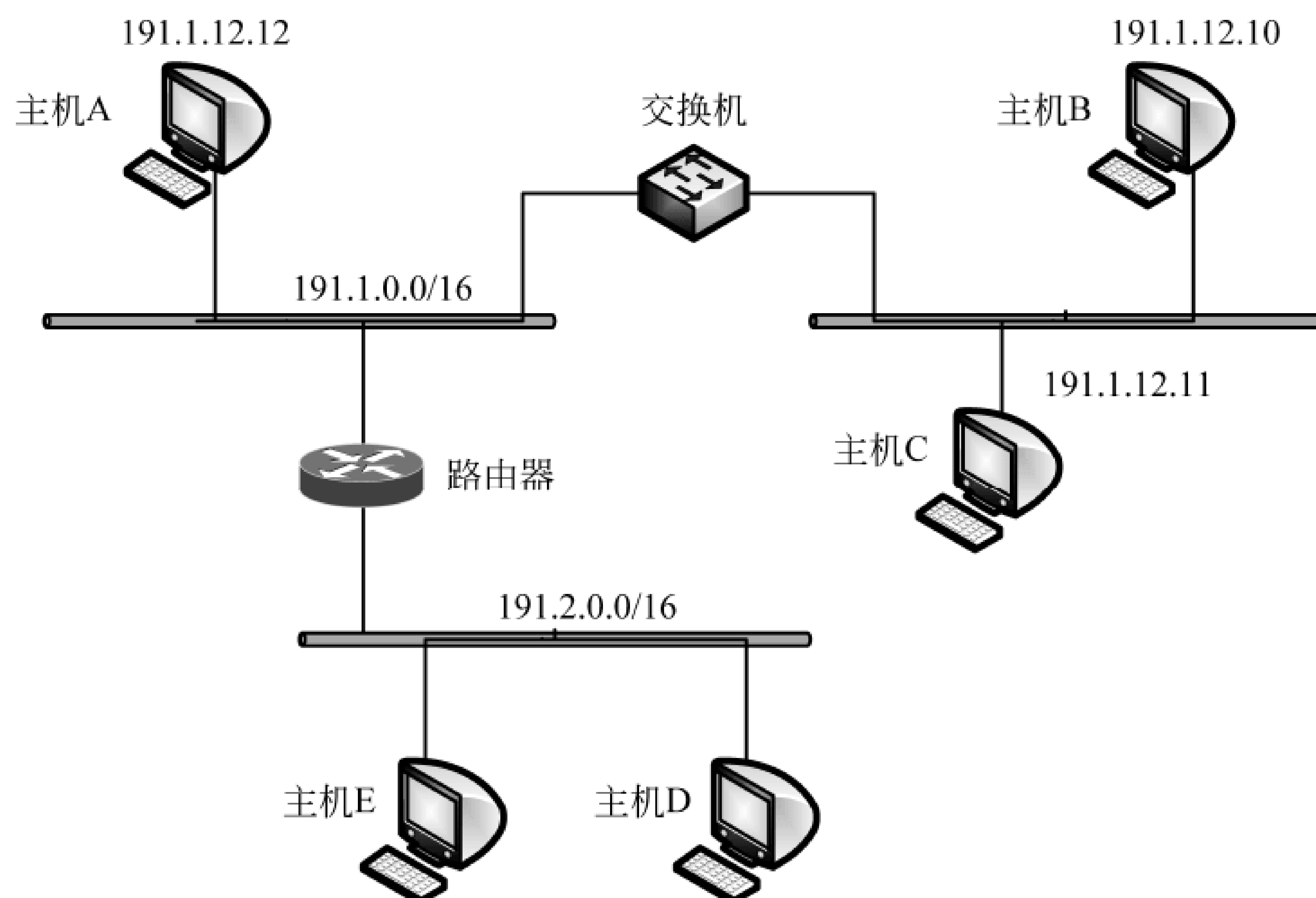
5-3-11 试指出以下哪个(或几个)IP 地址属于特殊地址,并比较它们的区别。

A. 221.1.25.255　　B. 255.255.255.255

C. 0.0.0.102　　D. 70.0.0.0

E. 127.1.2.3　　F. 10.1.2.3

5-3-12 网络结构如下图所示。请回答:



(1) 如果主机 A 发送一个目的地址为 255.255.255.255 的 IP 分组,哪些主机能够收到它?
(2) 如果主机 A 发送一个目的地址为 191.2.255.255 的 IP 分组,哪些主机能够收到它?
(3) 如果主机 A 发送一个目的地址为 0.0.12.10 的 IP 分组,哪些主机能够收到它?

5-3-13 主机的 IP 地址为 191.1.77.55,子网掩码为 255.255.252.0,那么它向其所在子网内发送广播分组,使用的目的地址为________。

A. 191.1.76.0　　B. 191.1.76.255
C. 191.1.77.255　　D. 191.1.79.255

5-3-14 网络地址为 169.1.8.0,没有划分子网。请指出该地址块的地址类型、IP 地址的范围、可以分配给主机的 IP 地址以及广播地址。

5-3-15 若 IP 地址为 191.230.34.56,子网掩码为 255.255.240.0。试求出子网号 subnet ID。

5-3-16 IP 地址为 129.240.80.20,子网掩码为 255.255.192.0。请用快捷方法计算出网络地址。

5-3-17 同一子网中两台主机的 IP 地址与子网掩码"相与"的结果是________。

A. 全 1　　B. 全 0　　C. 相同　　D. 不同

5-3-18 以下 IP 地址能够作为主机地址的是________。

A. 25.1.1.255　　B. 128.15.2.0
C. 193.2.220.256　　D. 127.0.0.0

5-3-19 一个 B 类地址掩码是 255.255.240.0,那么它每个子网的主机数为________。

A. 4096　　B. 4094　　C. 2048　　D. 1024

5-3-20 下列地址中属于 129.10.200.0/21 子网的地址是________。

A. 129.119.128.1　　B. 129.119.128.254
C. 129.120.207.254　　D. 129.120.208.1

5-3-21 以下 4 对 B 类地址中,属于同一子网的是________。

A. 180. 81.16.254/18 与 180. 81.32.254/18
B. 180. 81.16.254/18 与 180. 81.17.1/18
C. 180. 81.16.254/18 与 180. 81.33.1/18
D. 180. 81.17.254/18 与 180. 81.32.254/18

5-3-22 已知:A、B、C、D 共 4 台主机的 IP 地址分别为 210.20.1.112、210.20.1.120、210.20.1.135、210.20.1.202,子网掩码为 255.255.255.224。

求解:

(1) 4 台主机中哪些可以直接通信?哪些需要通过路由器才可以通信?
(2) 增加的主机 E 要与主机 D 直接通信,主机 E 的 IP 地址应该在哪个范围之内?
(3) 如果要使所有的主机都能够直接通信,需要对网络地址做什么样的调整?

5-3-23 如果用户希望将网络划分为 5 个子网,每个子网最多接入 20 台主机,那么以下 4 组掩码中最适合的是________。

A. 255.255.255.192　　B. 255.255.255.240

C. 255.255.255.224　　D. 255.255.255.248

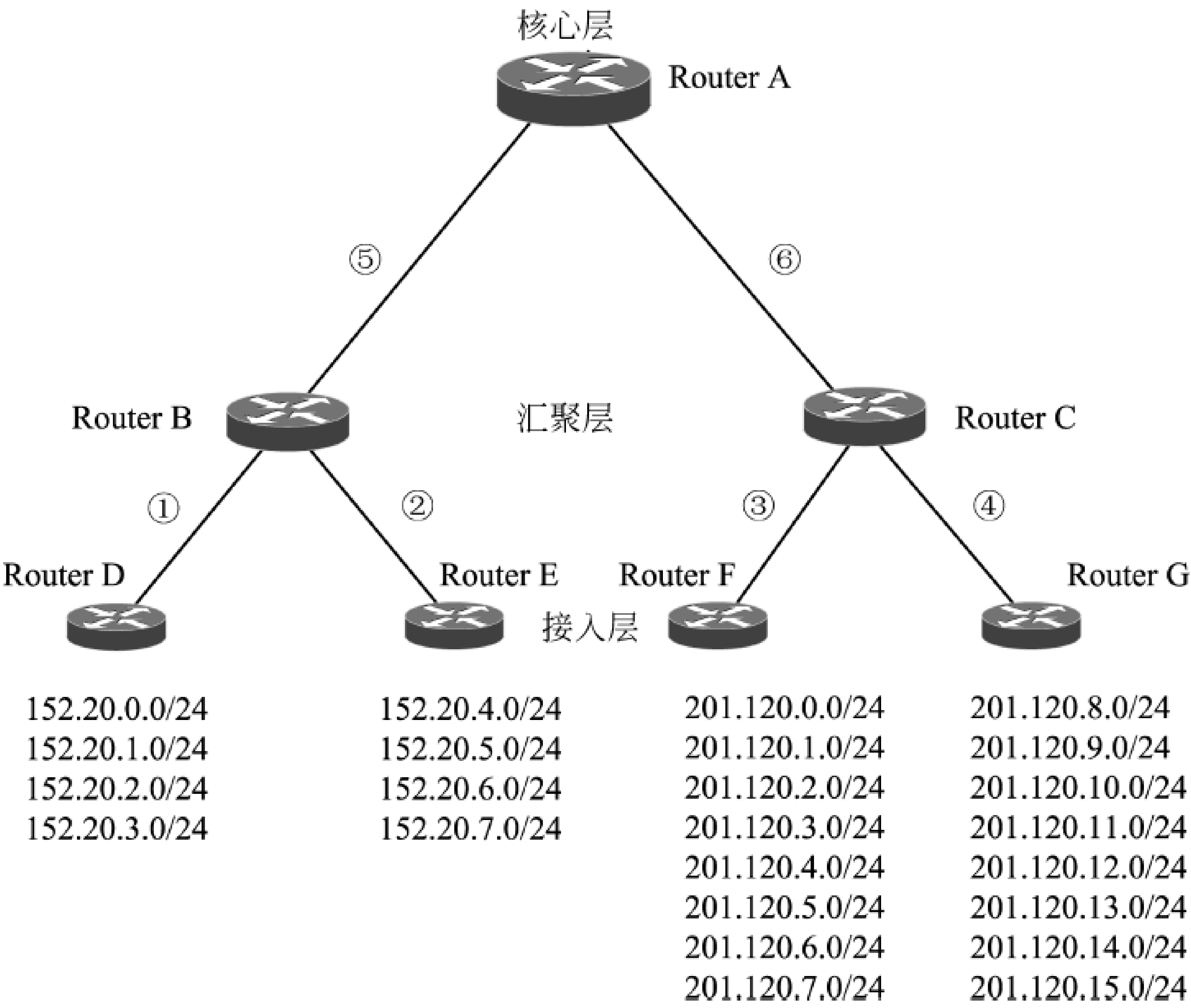
5-3-24 计算并填写下表。

IP 地址	129.10.179.7
子网掩码	255.255.192.0
地址类型	【1】
网络地址	【2】
直接广播地址	【3】
主机号	【4】
子网内的第一个可用 IP 地址	【5】

5-3-25 某个公司分到的 IP 地址为 181.55.0.0。该公司内部需要划分 1000 个子网。请设计这个子网的地址。

5-3-26 某个公司申请了一个整个 C 类 202.60.31.0 的 IP 地址空间。该公司有 100 名员工在销售部门工作，50 名员工在财务部门工作，50 名员工在设计部门工作。要求为销售部门、财务部门与设计部门分别组建子网。请按照用户需求划分地址范围。

5-3-27 一个简化的城域网结构如下图所示。请写出位于汇聚层、核心层等①～⑥共 6 个位置汇聚后的网络地址。



5-3-28 已知 4 个超网的 IP 地址为：

202.10.4.0/24

202.10.5.0/24

202.10.5.0/24

202.10.7.0/24

计算汇聚后的网络地址。

5-3-29 一台主机 IP 地址为 11.1.1.100,子网掩码为 255.0.0.0。用户需要给主机配置一个默认路由。与主机直接连接的路由器有 4 个 IP 地址与掩码:

Ⅰ. 11.1.1.1,255.0.0.0　　Ⅱ. 11.1.2.1,255.0.0.0

Ⅲ. 12.1.1.1,255.0.0.0　　Ⅳ. 13.1.2.1,255.0.0.0

以下选项中可能是该主机默认路由的是________。

A. Ⅰ和Ⅱ　　B. Ⅱ和Ⅲ

C. Ⅲ和Ⅳ　　D. Ⅳ和Ⅰ

5-3-30 对 4 条路由 191.18.129.0/24、191.18.129.0/24、191.18.129.0/24、191.18.129.0/24 进行聚合。以下能够覆盖聚合路由的地址是________。

A. 191.18.128.0/21　　B. 191.18.128.0/22

C. 191.18.130.0/22　　D. 191.18.132.0/23

5-3-31 以下关于 IP 地址 192.168.0.0～192.168.255.255 的描述中,正确的是________。

A. 保留的专用 IP 地址

B. 任何企业网络不能使用

C. 不能够在 Internet 上路由

D. 只能供 Internet 的 NIC 内部网络使用

5-3-32 以下 IP 地址中属于单播地址的是________。

A. 172.31.128.255/18　　B. 10.255.255.255

C. 192.168.24.59/30　　D. 224.105.5.211

5-3-33 路由器收到目的地址为 212.26.17.4 的分组,应转发的子网地址是________。

A. 212.26.0.0/21　　B. 212.26.16.0/20

C. 212.26.8.0/22　　D. 212.26.20.0/22

5-3-34 以下关于网络地址转换 NAT 特点的描述中,错误的是________。

A. NAT 的基本思路是 IP 地址重用,以缓解 IP 地址短缺问题

B. 内部网络的主机分配专用 IP 地址

C. NAT 路由器实行内部网络内部专用 IP 地址与全局 IP 地址的转换

D. NAT 属于一种静态地址转换方法

5.4 路由选择算法与分组交付

5-4-1 以下关于路由选择算法概念的描述中,错误的是________。

A. "路由选择"是指为转发的分组选择一条到达目的主机的"合理"路径

B. "路由选择算法"为路由器生成和更新路由表提供算法依据

C. 路由选择算法应能够适应网络拓扑和通信量的变化

D. "开销"一般是指传输过程的通信费用

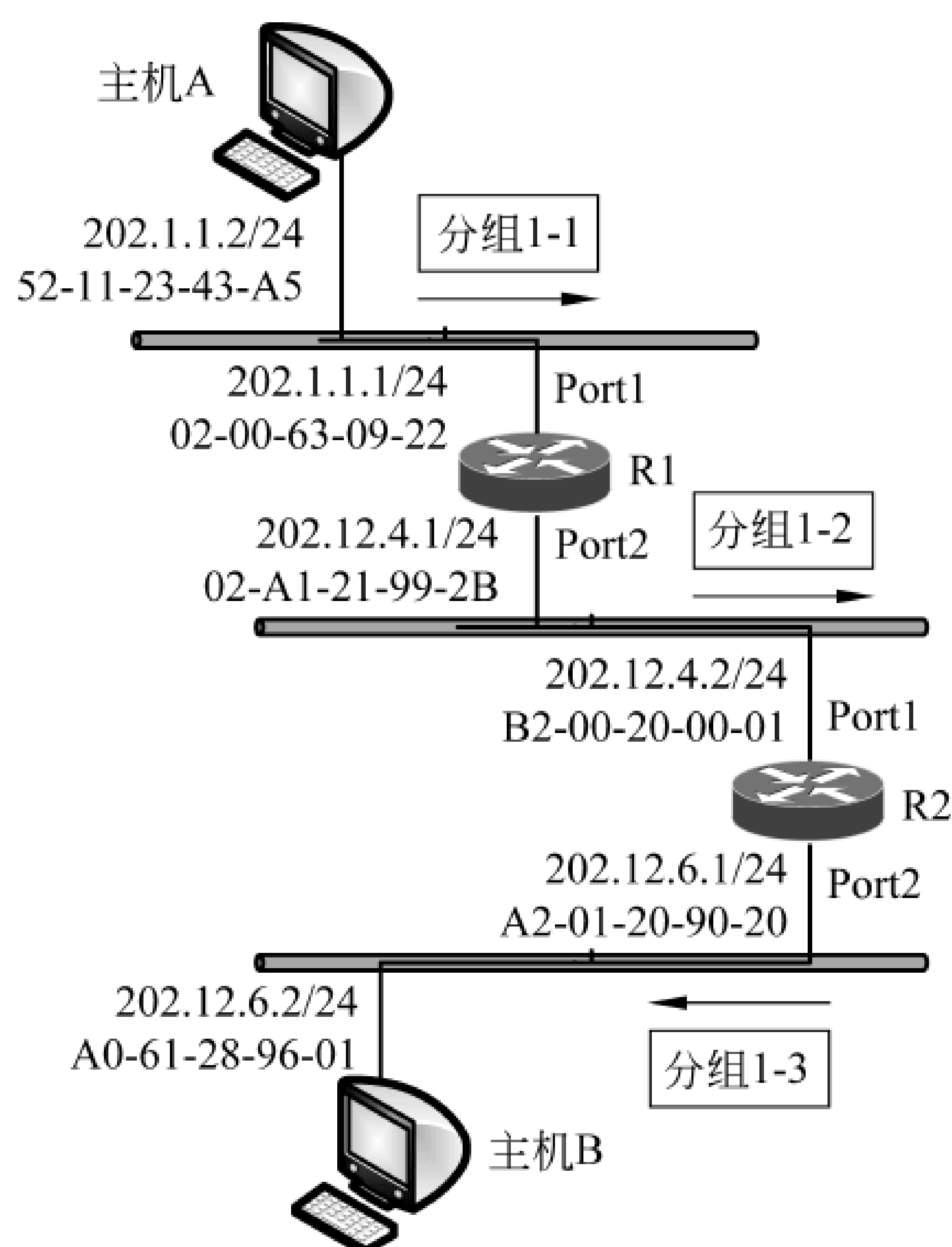
5-4-2 以下关于分组交付的描述中,错误的是________。

A. 分组交付是指网络中路由器或网桥转发 IP 分组的传输过程与转发机制

B. 分组交付要根据分组的源 IP 地址与目的 IP 地址来决定
C. 同一子网的主机之间交换 IP 分组属于直接交付
D. 不属于同一子网的 IP 分组交换属于间接交付

5-4-3 以下关于路由器组成和功能的描述中,错误的是________。
A. 路由器在数据链路层或网络层实现网络的互联
B. 路由器的主要服务功能是:建立并维护路由表,提供网络间的分组转发功能
C. 只要路由器接收分组、处理分组、输出分组的速率小于线速,无论是输入端口、处理分组过程与输出端口都会出现排队等待
D. 第三层交换机是用硬件实现的一种高速路由器

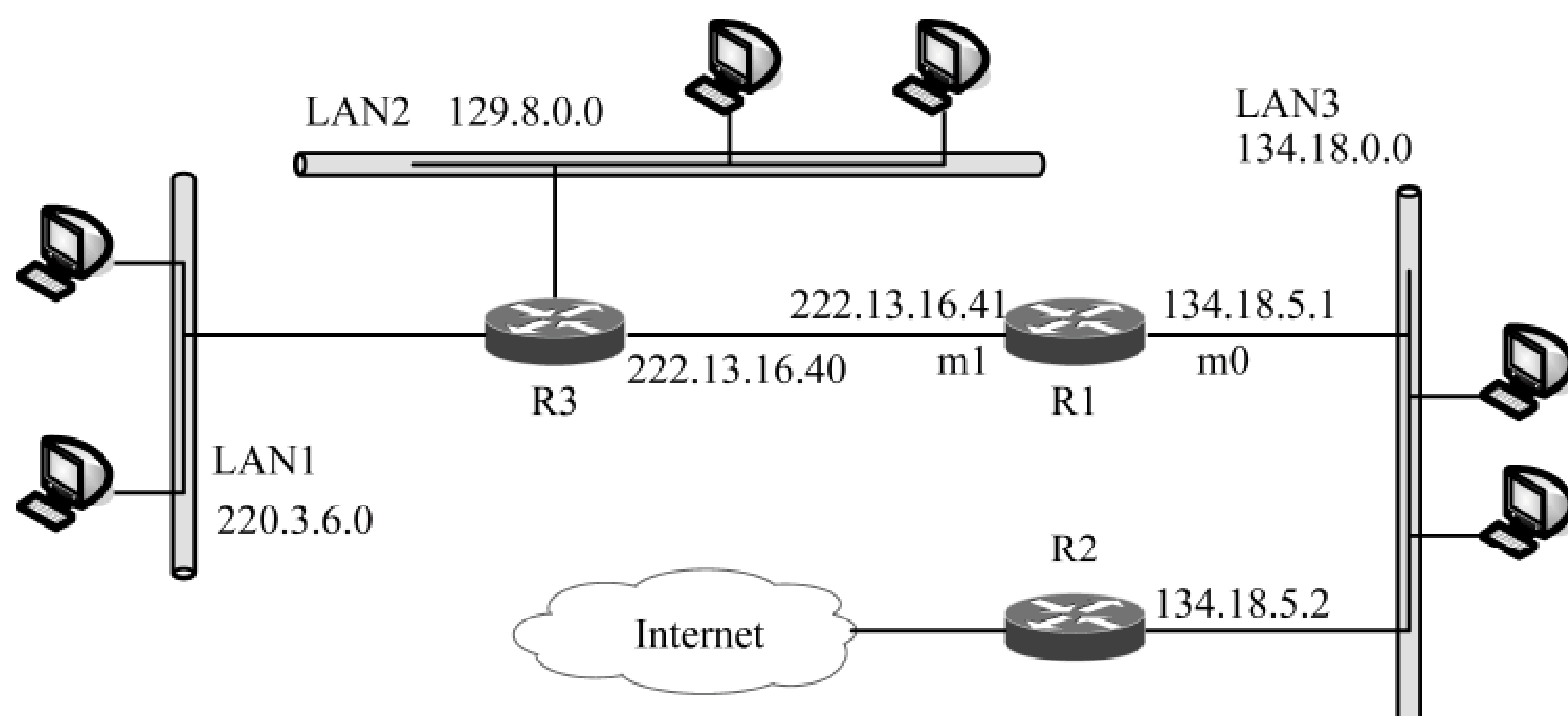
5-4-4 下图是主机 A 发送的分组通过路由器转发到主机 B 的过程示意图。



根据图中给出的信息,数据包经过路由器 R1 转发之后的分组 1-2 中的目的 IP 地址与目的 MAC 地址分别是________。

A. 202.12.4.1 和 02-A1-21-99-2B　　B. 202.12.5.2 和 B2-00-20-00-01
C. 202.12.4.2 和 A2-01-20-90-20　　D. 202.12.5.1 和 B2-00-20-00-01

5-4-5 根据下图所示的网络结构与地址,构造路由器 R1 的路由表。



5-4-6 路由器 A 的路由表如下表所示。请确定进入路由器 A 的 IP 地址为 132.19.237.5 分组的最佳路由。

路由器 A 的路由表

网　　络	输出端口
132.0.0.0/8	S0
132.19.0.0/11	E1
132.19.233.0/22	E2

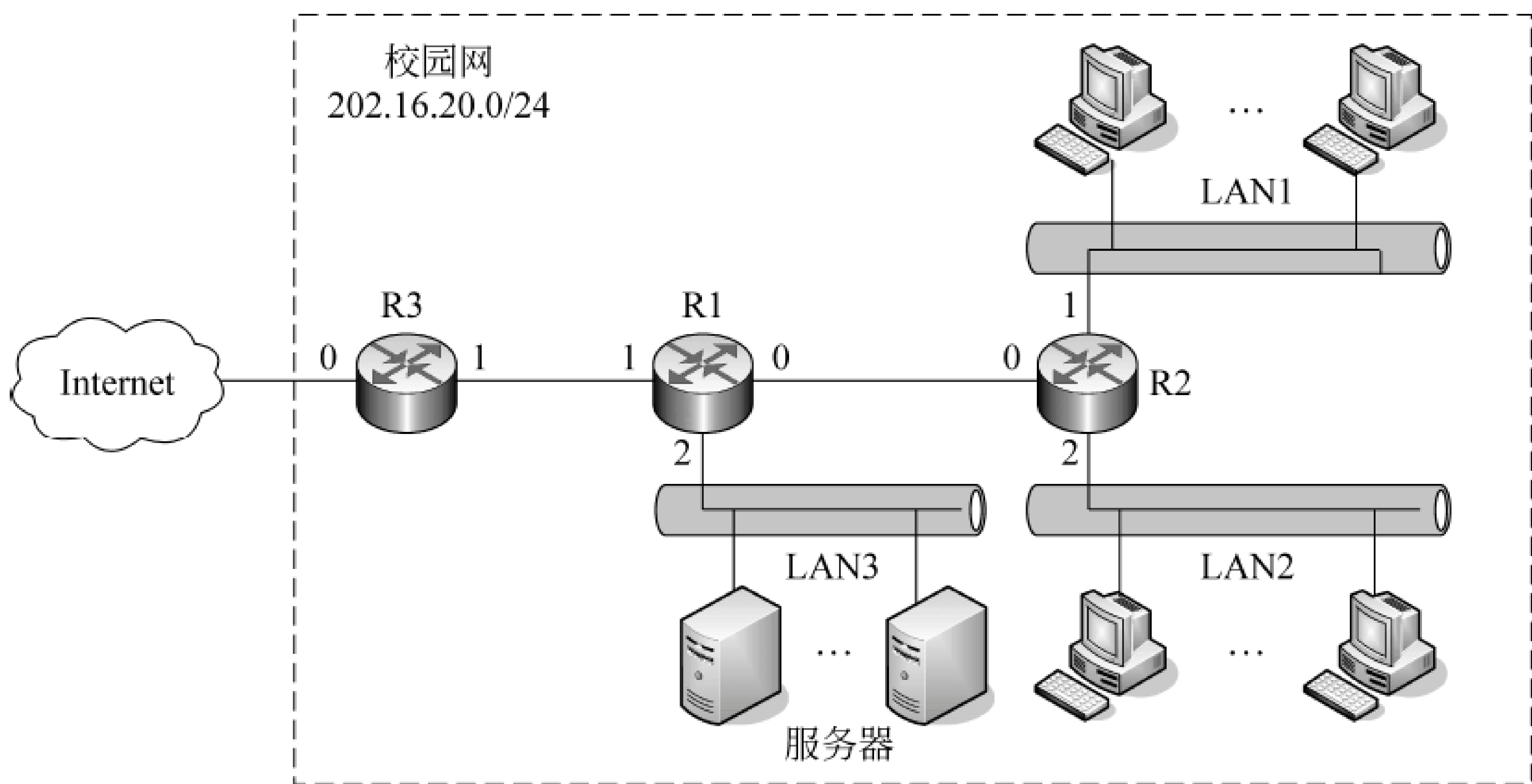
5-4-7 下图给出了一个小型校园网的网络结构。已知：校园网获得了一个 202.15.20.0/24 的 C 类 IP 地址；LAN1、LAN2 与 LAN3 各有最多为 60 台计算机或服务器；路由器 3 通过市教育科研网中心接入 Internet。

回答以下问题：

(1) 子网划分后的 LAN1、LAN2、LAN3 的主机 IP 地址范围。

(2) 路由器 R2 的路由表。

(3) 路由器 R1 聚合后的路由表。



5-4-8 路由器的路由表如下表所示。

路由表

网络地址/前缀	下一跳 IP 地址
142.150.64.0/24	A
142.150.71.128/28	B
142.150.71.128/30	C
142.150.0.0/16	D

请回答以下问题：

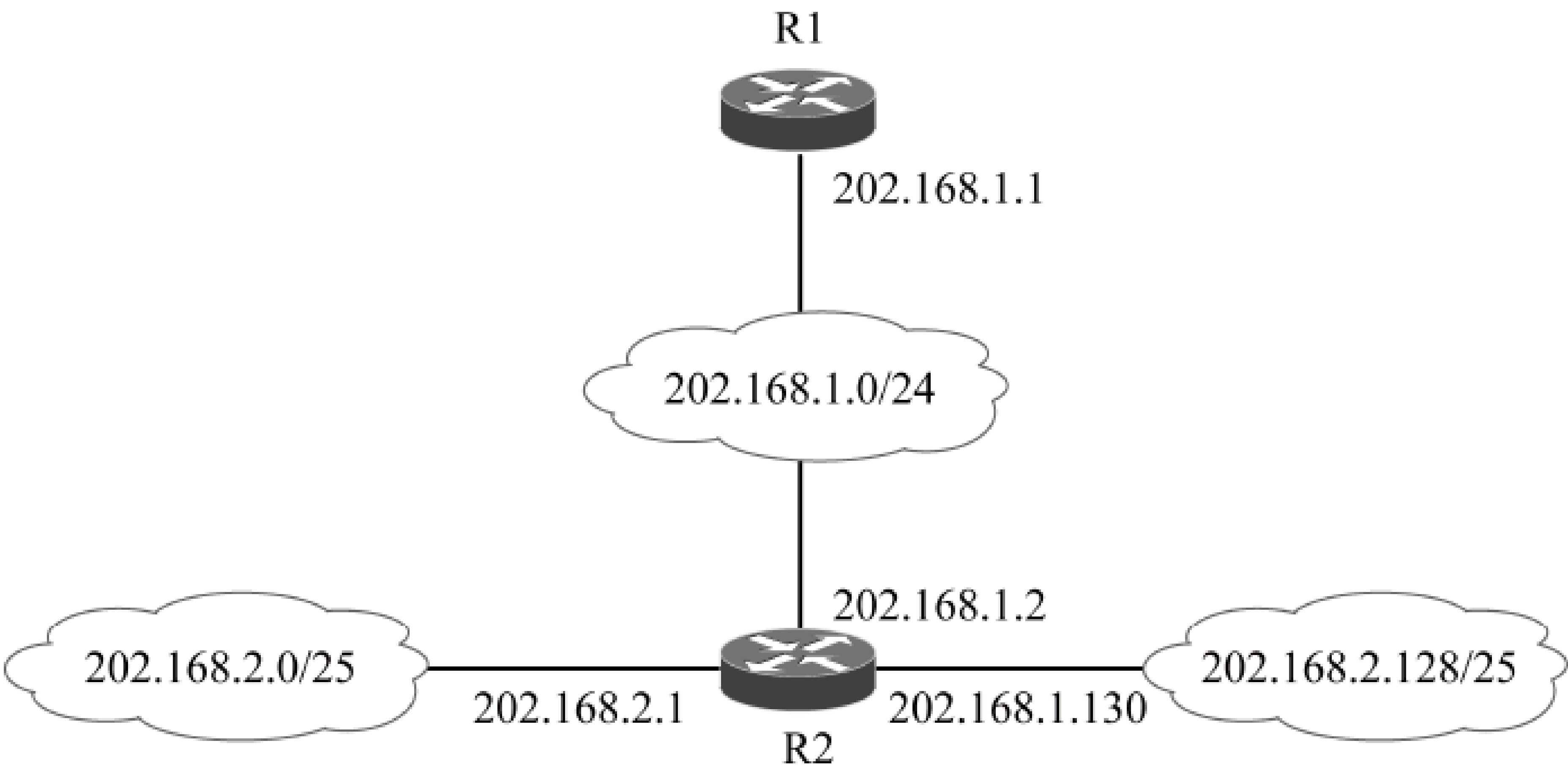
(1) 如果路由器接收到一个目的地址为 142.150.71.132 的 IP 分组，路由器为给分组选择的下一跳的输出端口，并说明理由。

(2) 如果在路由表中增加一条表项,使得142.150.71.132为目的地址的分组选择A作为下一跳的输出端口,并且不影响其他目的地址IP分组的转发。

(3) 在路由表中增加一个表项,使得所有目的地址与路由表中表项不匹配的IP分组的下一跳都是E。

(4) 将142.150.64.0/24划分为4个规模尽可能长的等长子网,给出子网掩码以及每个子网可以分配的地址范围。

5-4-9 网络拓扑如下图所示。路由器R1只有到达子网202.168.1.0/24的路由。为了使R1能够将IP分组传送到图中所有的子网,需要在R1路由表中增加一项路由(目的网络、子网掩码、下一跳)。请写出这条路由。



5-4-10 路由器不完整的路由表如下表所示。

序号	目的网络	子网掩码	下一跳	转发端口
1	176.11.64.0	255.255.240.0	R1端口1	端口2
2	176.11.16.0	255.255.240.0	直接交付	端口1
3	176.11.32.0	255.255.240.0	直接交付	端口2
4	176.11.48.0	255.255.240.0	直接交付	端口3
5	0.0.0.0	0.0.0.0	R2端口2	端口1

路由器R接收到以下分别发往6个目的主机的分组。

H1:21.13.24.78

H2:176.11.64.129

H3:176.11.35.72

H4:176.11.31.168

H5:176.11.60.239

H6:192.36.8.73

回答以下问题:

(1) 表中序号1~4的目的地址属于哪类网络?它们是由哪个网络中划分出来的?

(2) 若路由器R1端口1与路由器2端口2连接了主机号均为5,它的IP地址是什么?

(3) 目的主机 H1～H6 的下一跳地址是什么?

5-4-11 以下关于路由选择算法分类的描述中,错误的是________。

A. 路由选择算法分为静态与动态两类

B. 静态路由表是由人工方式建立与更新

C. 动态路由选择算法也称为自适应路由选择算法

D. 所有连接在互联网络中的主机和路由器的路由表都必须是动态的

5-4-12 以下关于距离-向量路由算法特点的描述中,错误的是________。

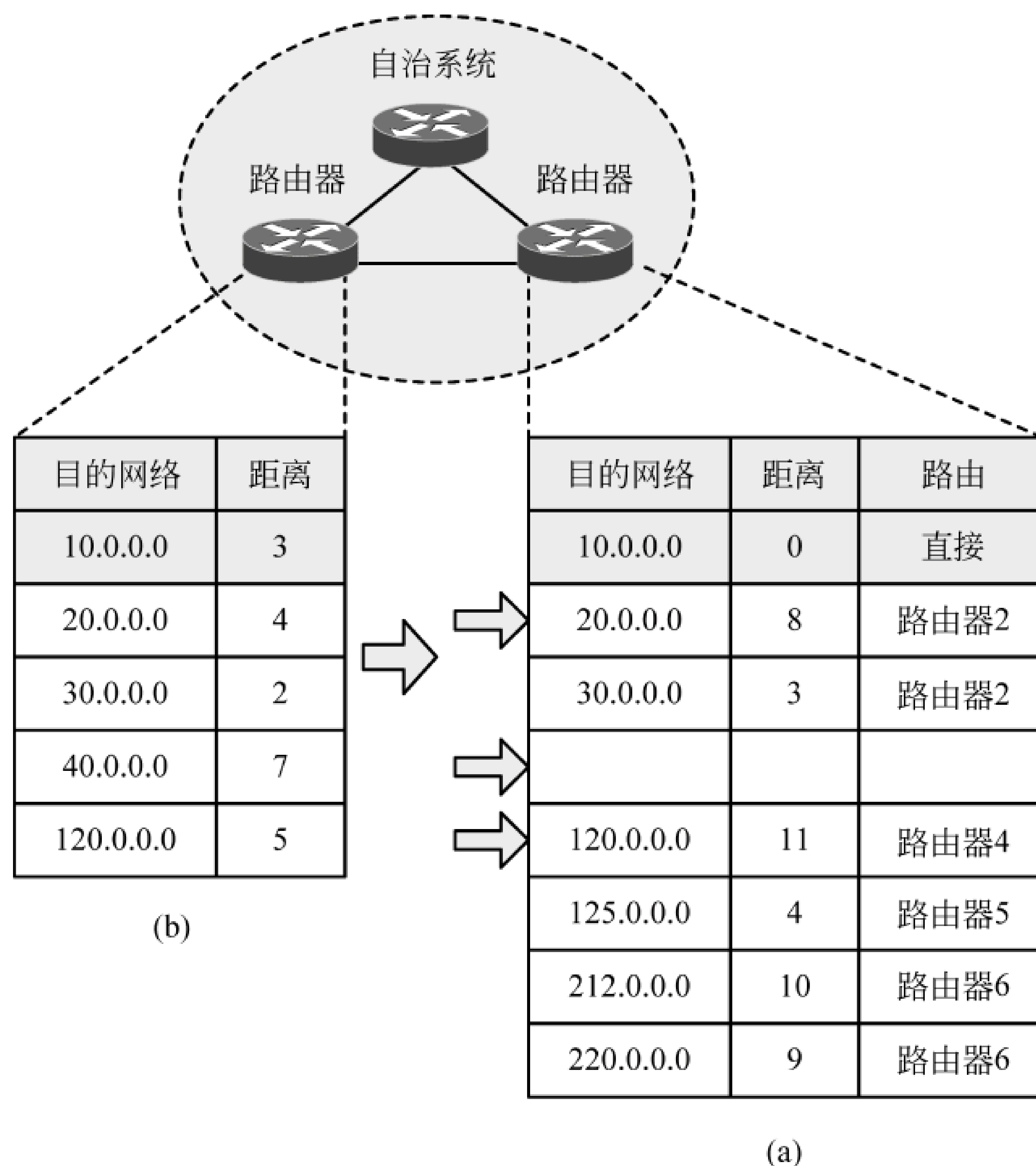
A. 距离-向量路由算法对跳数没有限制

B. Bellman-Ford 算法是一种典型的距离-向量路由算法

C. 路由表中记录当前已知的到每个目的网络输出端口与跳数

D. 通过与网络中相邻的路由器交换的路由信息来实现路由表的更新

5-4-13 距离-向量协议工作过程如下图所示。图中表(a)为路由器 1 初始的路由表;图中表(b)是相邻的路由器 2 传送来的路由表。请写出路由器 1 更新后的路由表。



目的网络	距离
10.0.0.0	3
20.0.0.0	4
30.0.0.0	2
40.0.0.0	7
120.0.0.0	5

(b)

目的网络	距离	路由
10.0.0.0	0	直接
20.0.0.0	8	路由器2
30.0.0.0	3	路由器2
120.0.0.0	11	路由器4
125.0.0.0	4	路由器5
212.0.0.0	10	路由器6
220.0.0.0	9	路由器6

(a)

5-4-14 以下关于路由器执行链路状态路由算法过程的描述中,错误的是________。

A. 构造一个分组,分组中包含所有刚得到的路由信息

B. 发现相邻路由器,并知道它们的 IP 地址

C. 测量到各个相邻路由器的延时或开销

D. 将这个分组发送给相邻的路由器

5-4-15 以下关于分层路由概念的描述中,错误的是________。

A. 为了适应网络规模扩大的需要,有必要采取分层路由的方法

B. 对于大型网络系统,可以采取多层路由的划分方法

C. 一个包含 N 个路由器的网络,最优的级数为 $\ln N$

D. 由于分层导致的平均路径长度的增长通常很大

5-4-16 以下关于自治系统基本概念的描述中,错误的是________。

A. Internet 采用分层的路由选择协议

B. 自治系统的核心是路由的"自治"

C. 将整个网络划分为许多较小的自治系统

D. 自治系统内部的路由器要了解整个互联网络的路由信息

5-4-17 以下关于域内路由与域间路由的描述中,错误的是________。

A. 自治系统内部的路由选择称为域内路由选择

B. 自治系统之间的路由选择称为域间路由选择

C. 路由选择协议分为两大类:内部网关协议(IGP)、外部网关协议(EGP)

D. 路由信息协议 RIP 用于外部网关协议

5-4-18 以下关于 RIP 与距离向量路由选择的描述中,错误的是________。

A. RIP 要求路由器都要维护从它到每个内部路由器的距离向量

B. 路由表更新的原则是找出到达每个网络的最短距离

C. 与路由器直接连接的网络的距离值为 0

D. 每经过一个路由器,距离值加 1

5-4-19 自治系统内采用 RIP 协议,路由器 R1 收到邻居节点路由器 R2 的距离向量中包括信息〈net1,16〉,那么可以得出的结论是________。

A. R2 可以经过 R1 到达 net1,跳数为 16

B. R2 可以经过 R1 到达 net1,跳数为 17

C. R1 可以经过 R2 到达 net1,跳数为 17

D. R1 不能经过 R2 到达 net1

5-4-20 以下关于 OSPF 协议特征的描述中,错误的是________。

A. 域之间通过区域边界路由器互联

B. 主干路由器不能够兼做区域边界路由器

C. OSPF 协议将一个自治系统划分成若干个域,有一个特殊的域叫作主干域

D. 自治系统包括区域内部路由器、主干路由器、区域边界路由器与 AS 边界路由器

5-4-21 以下关于 OSPF 协议与链路状态协议的描述中,错误的是________。

A. OSPF 通过链路状态协议实现 AS 内部路由表更新

B. 链路状态"度量"可以是距离、带宽、延时或费用等

C. 链路状态协议要求定时向 AS 中其他路由器发送路由信息

D. 链路状态协议要求每个路由器采用洪泛方法向 AS 中其他的路由器发送路由信息

5-4-22 以下关于 BGP 协议特征的描述中,错误的是________。

A. BGP 的路由选择算法是基于路径向量算法

B. BGP 路由器的路由表要包括分组到达目的网络的路径

C. BGP 要求相邻的 AS 边界路由器之间交换到达目的网络的路径

D. BGP 要求相邻的 AS 边界路由器在路径发生变化时交换路由信息

5-4-23 RIP、OSPF 与 BGP 协议的报文是用 IP 分组、UDP 报文或 TCP 报文封装的吗？请从所使用的 IP 协议的“协议”字段与 UDP、TCP“熟知端口号”来说明判断的依据。

* **5-4-24** 请说明 RIP、OSPF 与 BGP 协议在“路由信息更新周期”与判断“路由记录”方面的差异。

5.5 互联网控制报文协议 ICMP

5-5-1 以下关于 ICMP 协议的描述中，错误的是________。

A. IP 协议缺乏差错控制与查询机制

B. 差错报告采用路由器-源主机的模式

C. ICMP 报文分成差错报告与查询报文

D. 作为 IP 协议的补充，ICMP 报文直接封装在 Ethernet 帧中

5-5-2 以下关于 ICMP 特点的描述中错误的是________。

A. ICMP 是传输层的一个协议

B. ICMP 发送时要封装成 IP 分组

C. ICMP 由路由器向源主机报告传输出错原因

D. ICMP 只是要解决 IP 协议可能出现的不可靠问题

5-5-3 以下关于 ICMP 报文结构的描述中，错误的是________。

A. TCP 报文头中协议字段值为 1 表示网络层数据部分是 ICMP 报文

B. ICMP 报文的前 4B 的格式是统一的

C. ICMP 报文的第三个字段(2B)是校验和

D. ICMP 报文的第四个字段(4B)的内容与类型相关

5-5-4 因拥塞而丢弃分组，路由器向源主机发出的 ICMP 报文类型是________。

A. 重定向　　B. 源抑制　　C. 超时　　D. 目的不可达

5-5-5 以下关于 ICMP 不同类型的“目的不可达”报文的描述中，错误的是________。

A. 目的不可达报文是指：路由器寻址出错

B. 主机不可达是指：可能是目的主机不工作或不存在

C. 协议不可达是指：分组要交付的应用进程没有运行

D. 目的网络不可知是指：路由器根本不知道关于目的网络的信息

5-5-6 以下关于 ICMP 目的不可达报文不是由路由器发出的是________。

A. 源路由选择不能完成

B. 源主机抑制

C. 端口不可达

D. 目的网络不可知

5.6 IP 多播与 IGMP 协议

5-6-1 以下关于多播概念的描述中，错误的是________。

A. IP 多播是指多个接收者可以接收到从同一个或一组源节点发送的相同内容的分组

B. 发送主机使用多播地址发送分组时不需要了解接收者的位置信息与状态信息

C. 利用多播树可以将多播分组转发到整个互联网
D. 支持多播协议的路由器叫作多播路由器

5-6-2 以下关于多播主干 MBONE 的描述中,错误的是________。
A. 在 Internet 中只有一小部分是能够支持多播协议的多播路由器
B. 在邻近找不到其他多播路由器的困难时的最好办法是采用隧道技术
C. 利用隧道技术的概念,可以在孤立的多播路由器之外改造一个多播主干
D. 将多播分组封装在单播分组中,改变单播分组的 IP 地址,就可以建立逻辑隧道

5-6-3 以下关于 IP 多播地址的描述中,错误的是________。
A. D 类 IP 地址可以用于多播地址
B. 多播地址可以用于目的地址与源地址
C. D 类 IP 地址的范围在 224.0.0.0～224.255.255.255
D. IP 多播协议支持两类多播地址：永久组地址与临时组地址

5-6-4 以下关于多播路由选择概念的描述中,错误的是________。
A. 为了有效地进行多播,需要建立一个由源节点为根,组成员为树叶的支撑树
B. 采用组共享树方法时,系统中有 N 个组,那么最多有 $N\times(N-1)$个树
C. 采用源端基准树方法时,源端与组的组合决定树的结构
D. 支撑树从根到树叶的每个路径都是可能的最短路径

5.7 MPLS 协议

5-7-1 以下关于拥塞控制概念的描述中,错误的是________。
A. 当一个子网或子网的一部分出现过多的分组造成网络性能下降的现象称为拥塞
B. 流量控制与特定的发送方和接收方之间的点对点流量是一个局部性的问题
C. 拥塞控制是确保子网能承受所有到达的分组流量是一个全局性的问题
D. 显式反馈算法由源节点通过检测来判断是否出现拥塞

5-7-2 以下关于 QoS 概念的描述中,错误的是________。
A. 网络中从源节点到目的节点的分组流称为一个流
B. 表述 QoS 的参数主要是可靠性、延时、延时抖动与带宽
C. RSVP 根据服务类型提供不同网络资源,以保证 IP 分组的传输服务质量
D. MPLS 提供面向连接的服务、动态定义路由、支持 VPN 与支持多种网络层协议

5.8 地址解析协议

5-8-1 以下关于 ARP 概念的描述中,错误的是________。
A. 主机和路由器在数据链路层用 MAC 地址来标识
B. 在主机或路由器中必须有一张“IP 地址-物理地址对照表”
C. 从 MAC 地址找出对应的 IP 地址的映射过程称为反向地址解析
D. 主机只有通过“静态映射”方法才能获取与 IP 地址相对应的 MAC 地址

5-8-2 ARP 的功能是________。
A. 根据 IP 地址查询 MAC 地址
B. 根据 MAC 地址查询 IP 地址

C. 根据 IP 地址查询端口号

D. 根据 IP 地址查询域名

5-8-3 以下关于 ARP 协议的描述中，错误的是________。

A. ARP 请求分组的目的 MAC 地址字段写入 FF

B. ARP 请求分组以广播地址作为目的地址发送出去

C. 根据已知的 IP 地址找出对应 MAC 地址的映射过程叫作地址解析

D. 如果不知道发送分组的目的 IP 地址对应的目的 MAC 地址，则需要进行地址解析

* **5-8-4** 某路由器的 IP 地址为 125.45.23.12，MAC 地址为 23-45-AB-4F-67-CD。路由器接收到目的地址为 125.11.78.10 的分组。参照下面的 ARP 分组结构与 Ethernet 帧结构。

<table>
<tr><td colspan="2">硬件类型</td><td colspan="2">协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议地址长度</td><td colspan="2">操作类型</td></tr>
<tr><td colspan="4">源MAC地址</td></tr>
<tr><td colspan="2">源MAC地址</td><td colspan="2">目的MAC地址(全0)</td></tr>
<tr><td colspan="4">目的MAC地址(全0)</td></tr>
<tr><td colspan="4">目的IP地址</td></tr>
</table>

ARP报文结构

SFD	目的地址	源地址	数据	FCS
8B	6B	6B	46~1500B	4B

Ethernet帧结构

求解以下问题：

(1) 给出路由器发出的 ARP 请求分组中各项的数据（假设不划分子网）。

(2) 如果目的主机的 MAC 地址为 AA-BB-BA-A2-4F-67-CD。试给出 ARP 响应分组各项的数据。

(3) 将问题(1)的结果封装成数据链路层的帧。

(4) 将问题(2)的结果封装成数据链路层的帧。

5.9 移动 IP 协议

5-9-1 以下关于移动 IP 基本术语的描述中，错误的是________。

A. 家乡代理通过隧道将发送给移动节点的 IP 分组转发到移动节点

B. 转交地址是指当移动节点接入一个外地网络时使用的、长期有效的 IP 地址

C. 目的地址为家乡地址的 IP 分组，将会以标准的 IP 路由机制发送到家乡网络

D. 家乡链路与外地链路比家乡网络与外地网络更精确地表示出移动节点接入的位置

5-9-2 以下关于移动 IPv4 工作原理的描述中，错误的是________。

A. 移动 IP 的分组路由可以分为单播、广播与多播

B. 移动 IPv4 代理发现是通过扩展 IGMP 路由发现机制来实现

C. 移动节点到达新的网络后,通过注册过程将自己新的可达信息通知家乡代理

D. 移动IPv4的工作过程可以分为4个阶段:代理发现、注册、分组路由与注销

5.10 IPv6协议

5-10-1 以下关于IPv6与IPv4报头比较的描述中,错误的是________。

A. IPv6取消了头部长度字段是因为头部长度是定长的

B. IPv6取消了总长度字段,替代的是有效片偏移值

C. IPv6用跳步限制字段取代IPv4的生存周期字段

D. IPv4的报头选项放到IPv6的扩展头部

5-10-2 以下关于IPv4过渡到IPv6方法的描述中,错误的是________。

A. 双IP协议层就是双协议栈方案

B. 双协议栈的方案是:一个节点同时运行IPv4与IPv6协议

C. 两台IPv6主机要通过IPv4网络传输数据时可以使用隧道技术

D. 隧道配置可以分为路由器-路由器、主机-主机、主机-路由器或路由器-主机

5-10-3 以下关于IPv6地址“1A22:120D:0000:0000:72A2:0000:0000:00C0”的不同表示方法中,错误的是________。

A. 1A22:120D::72A2:0000:0000:00C0

B. 1A22:120D::72A2:0:0:C0

C. 1A22:120D::72A2::00C0

D. 1A22:120D:0:0:72A2::C0

5-10-4 IPv6地址FF02:3::5:1的::之间被压缩了多少位0?

第二部分　同步练习答案与解析

5.1 网络层与IP协议

5-1-1 分析:设计该例题的目的是加深读者对网络层基本概念的理解。在讨论网络层基本概念时,需要注意以下几个主要问题:

(1) 网络层要实现路由选择、拥塞控制与网络互联等基本功能。

(2) 网络层使用了数据链路层的服务,向传输层端一端的传输连接提供服务。

(3) 网络层服务应独立于通信子网所采用的技术。

(4) 网络层向传输层提供的服务不应受通信子网的数量、类型与拓扑构型的影响。

(5) 网络层具有跨局域网、城域网与广域网的互联网络寻址能力。

从以上分析中可以看出,B对网络层与低层传输技术关系的描述是错误的。

答案:B。

5-1-2 分析:设计该例题的目的是加深读者对异构网络互联的理解。在讨论异构网络互联时,需要注意以下几个主要问题:

(1) 实际网络系统的互联必然要涉及异构性(heterogeneity)问题。异构性是指网络和通信协议、计算机硬件和操作系统的差异性。

(2) 网络互联的异构性主要表现在:

① 不同类型的网络(广域网、城域网、局域网等)。

② 使用不同类型通信协议的网络(Ethernet、Token Ring、ATM 等)。

③ 不同类型的计算机系统(大型机、小型机、工作站与微型机等)。

④ 使用不同类型操作系统的计算机(Windows、UNIX、OS/2 与 Linux 等)。

(3) 利用路由器将两个或两个以上的网络互联起来构成的系统叫作互联网络。

(4) 通常意义上的互联网络(internet)与因特网(Internet)是不同的。Internet 是网络互联技术发展与应用的产物,是一种覆盖世界范围的大型网际网。

从以上分析中可以看出,D 描述的利用集线器级联方法组建的是规模比较大的局域网,不属于网络的互联,因此这种提法是错误的。

答案:D。

5.2 IPv4 协议的基本内容

5-2-1 分析:设计该例题的目的是加深读者对 IP 协议的特点的理解。在讨论 IP 协议的特点时,需要注意以下几个主要问题:

(1) IP 协议是一种无连接、不可靠的分组传送服务的协议,它不提供对分组严格的差错校验和传输过程的跟踪。因此它提供的是一种尽力而为(best-effort)的服务。

(2) 无连接(connectionless)意味着 IP 协议并不维护 IP 分组发送后的任何状态信息。每个分组的传输过程是相互独立的。

(3) 不可靠(unreliable)意味着 IP 协议不能保证每个 IP 分组都能正确的、不丢失和顺序地到达目的节点。

(4) IP 协议是点-点的网络层通信协议。IP 协议是针对源主机-路由器、路由器-路由器、路由器-主机之间的数据传输的点-点的网络层通信协议。

(5) IP 协议向传输层屏蔽了物理网络的差异。作为一个面向互联网的网络层协议,它必然要面对各种异构的网络和协议。协议的设计者希望使用 IP 分组来统一不同的网络帧。

从以上分析中可以看出,IP 协议提供的面向无连接服务,表示它不维护 IP 分组发送后的任何状态信息,每个分组的传输过程是相互独立的。因此,C 的描述是错误的。

答案:C。

5-2-2 分析:设计该例题的目的是加深读者对 IP 分组结构的理解。在讨论 IP 分组结构时,需要注意以下几个主要问题:

(1) IP 分组是由分组头和数据两个部分。分组头长度是可变的。IP 分组头的基本长度是 20 个字节,选项最长为 40 个字节。

(2) IP 分组头包括版本字段、协议字段、长度字段、服务类型字段、生存时间字段、头校验和字段与地址字段。

(3) 版本字段表示 IP 协议版本。“版本”字段值为 4,表示 IPv4;“版本”字段值为 6,表示 IPv6。

(4) 协议字段表示使用 IP 协议的高层协议类型,如 TCP、UDP,以及 ICMP 或 IGMP 协议等。

(5) 分组头有两个长度字段:分组头长度和总长度。分组头长度字段值表示出以 4 个

字节为一个单位的分组头的长度。分组头长度字段最小值为 5,最大值为 15。总长度字段表示以字节为单位的分组头长度与数据长度之和。

(6) 服务类型字段表示服务类型与优先级。

(7) 生存时间(TTL)字段值表示一个分组从源节点到达目的节点可以经过的最多的路由器跳数(hops)。

(8) 头校验和用于保证分组头数据完整性。

(9) 地址字段包括源 IP 地址与目的 IP 地址。

从以上分析中可以看出,IP 分组的"协议字段"是表示使用 IP 协议的高层协议类型,而不是 IP 协议版本。因此,C 的描述是错误的。

答案:C。

5-2-3 分析:设计这个例题的目的是加深读者对 IPv4 报头结构和各个字段含义的理解。

(1) IPv4 报头的结构如图 5-1 所示。



图 5-1 IPv4 报头结构

(2) 本题讨论的是前 8 位,即版本与报头长度。版本与报头长度字段均为 4 位。版本字段值为 4 表示是 IPv4 协议;报头长度字段值是定义了以 4 字节为单位的报头长度。

答案:路由器接收到一个 IP 分组的前 8 位是 01000010。

(1) 第一个 4 位是 0100,转换为十进制数为 4,表示是 IPv4 协议,没有错误。

(2) 第二个 4 位是 0010,转换为十进制数为 2,表示是报头长度为 8(4×2)个字节,而 IPv4 的固定报头就是 20 个字节,因此该字段出现错误,应该丢弃。

5-2-4 分析:设计该例题的目的是检查读者对 IPv4 报头两个长度字段意义的理解。注意两个长度字段值定义的不同。

解:

(1) HLEN=5_{16},表示报头长度为 4×5=20 字节,等于 IPv4 的固定报头的长度,表示没有报头选项。

(2) 总长度字段值为 0028_{16},用十进制数表示为 40。总长度字段值表示以字节为单位的分组长度,这点与报头长度(HLEN)字段值的意义不同。因此,该分组的数据长度等于 40－20＝20(字节)。

答案:该分组携带了 20 字节的数据。

5-2-5 分析:设计该例题的目的是加深读者对校验和的理解。在讨论校验和时,需要注意以下几个主要问题:

(1) IPv4 分组头的校验和的设置是为了保证分组头部的数据完整性。

(2) IPv4 校验和字段长度为 8 位。

(3) IP 分组只对分组头进行校验和的计算,不包括分组数据部分。

(4) IP 分组头的部分字段数据(如生存时间 TTL、标志、片偏移等)经过一个路由器时发生的变化分两种情况。

一种情况是:如果分组长度不超过下一段链路的 MTU,那么路由器只需要将 TTL 值减 1,同时需要进行头校验和计算。

另一种情况是:如果分组长度超过下一段链路的 MTU,那么路由器就需要只需要将 TTL 值减 1,同时需要进行头校验和计算。

实际上,IP 分组头每经过一个路由器 TTL 值都一定会变化。

因此,B 的描述是错误的。

答案:B。

5-2-6 分析:设计该例题的目的是加深读者对 IP 分组分片基本方法的理解。在讨论 IP 分组分片基本方法时,需要注意以下几个主要问题:

(1) IP 分组长度大于 MTU 时,就必须对 IP 分组进行分片。

(2) 在 IP 分组的分组头中,与一个分组的分片与组装相关的是标识字段、标志字段与片偏移字段。

(3) 为了防止同一个分组的不同的片到达目的节点时出现乱序的现象,需要为一个分组的所有片分配一个字段标识 ID 值。

(4) 标志字段中不分片(DF)值为 1 表示接收节点不能对分组分片。如果分组的长度,超过 MTU,又不可以分片,那么这个分组只能丢弃,并要用 ICMP 差错报文向源主机报告。DF＝0,表示可以分片。分片 MF 值为 1 表示接收的分片不是最后的一个分片,MF 为 0 表示接收的是最后的一个分片。

(5) 片偏移值表示该分片在整个分组中的相对位置。片偏移值是以 8 字节为单位来计数的,因此选择的分片长度应该是 8 字节的整数倍。

需要注意的是,如果 DF＝1,分组的长度又超过 MTU,则丢弃该分组,但是需要用 ICMP 差错报文向源主机报告出错。因此,D 的描述是错误的。

答案:D。

5-2-7 分析:设计该例题的目的是加深读者对于分组头中标志(flag)字段与片偏移字段意义的理解。

解:到达的分组的 M＝1,表示该分组已经被分片。分片的偏移值为 0,表示这个分片是第一个分片。

答案:第一个分片。

5-2-8 分析：设计这道习题的目的是加深读者对 IP 分组在传输过程中分片的概念与方法。

解：已知：IP 分组头部长度为 20B，数据字段长度为 2000B。由于分组总长度都超过了两个网络的最大传输单元值，因此必须要分片。在分片过程中需要在每个分片的头部保留分组头部 20B。

(1) 经过第一个 MTU＝1500B 的网络，需要分为 2 个片。

P1＝1480B＋20B＝1500B

P2＝2000B－1480B＋20B＝540B

(2) 经过第二个 MTU＝576B 的网络，P1 需要继续分片。

P1－1＝556B＋20B＝576B

P1－2＝556B＋20B＝576B

P1－3＝1480B－556B－556B＋20B＝388B

P2＝540B<576B，不需要分片。

答案：

(1) 经过第一个网络时分为 2 个片，长度分别为：1500B、540B。

(2) 经过第二个网络时分为 4 个片，长度分别为：576B、576B、388B、540B。

5-2-9 分析：设计这道习题的目的是校验读者对 IPv4 分组头、分组转发原理的理解。回答这个问题需要注意组成 IPv4 分组头的相关字段的含义与特点。

(1) 版本字段表示所使用的网络层 IP 协议的版本号。在分组传输过程中是不变的。

(2) 协议字段表示使用 IP 协议的高层协议类型，如 TCP 或者是 UDP。在分组传输过程中是不变的。

(3) 长度字段。IPv4 分组头有两个长度字段：分组头长度(hlen)和总长度(total length)。在分组传输过程中是不变的。如果 IP 分组长度超过输出链路的 MTU，那么需要修改 IP 分组头中的总长度字段、标志字段、片偏移字段。

(4) 服务类型字段。服务类型字段由服务类型 TOS、优先级字段、1 位的保留位构成。在分组传输过程中是不变的。

(5) 地址(address)字段。读者在见到这道题目时，一般都会怀疑地址字段值是否会变化。其实，地址字段是很简单的。在分组的传输过程中，无论采用什么样的传输路径或如何分片，源地址与目的地址始终保持不变。

(6) 生存时间(TTL)字段。TTL 的初始值由源主机设置，经过一个路由器转发之后，TTL 值减 1。当 TTL 的值为 0 时，丢弃分组并发送 ICMP 报文通知源主机。因此，TTL 字段值在分组传输过程中是变化的。

(7) IP 分组作为网络层的数据必然通过数据链路层，封装成帧再通过物理层来传输。一个分组可能要经过多个不同的网络。每个路由器都要将接收的帧进行拆帧和处理，然后封装成其他类型的帧。帧的格式与长度取决于网络采用的协议。在 IP 分组头中，与分组的分片与组装相关的字段——标识、标志与片偏移就有可能发生变化。

(8) 头校验和是为了保证分组头部的数据完整性。IP 分组只对分组头进行校验，而不

包括分组数据。

答案：

如果 IP 分组长度不超过输出链路的 MTU，那么每经过一个路由器，生存时间(TTL)字段值每变化一次，头校验和就重新计算一次，头校验和字段的数值也变化一次。

如果 IP 分组长度超过输出链路的 MTU，那么需要修改 IP 分组头中的总长度字段、标志字段、片偏移字段、生存时间(TTL)字段与校验和字段。

5-2-10 分析：设计这道习题的目的是帮助读者理解 IP 分组长度的限制。

题中给出了 D 为可变，首先排除。在网络不同层次的协议数据单元 PDU 长度都有限制。网络不同层次常用的 PDU 长度中最大长度值从小到大排列是：TCP 报文段最大长度默认值为 536B；Ethernet 帧规定的最大长度为 1500B；IP 分组与 UDP 分组的最大值都是 65535B。因此，A 的描述是正确的。

答案：A。

5-2-11 分析：设计这道习题的目的是加深读者对 IP 分组头选项中源路由的理解。回答这个问题需要注意以下几点。

(1) 设置 IP 分组头选项主要用于控制与测试。分组头选项由 3 部分组成：选项码、长度与选项数据。选项码用于确定该选项的具体功能，例如源路由、记录路由、时间戳等。长度表示出选项数据的大小。

(2) 源路由是指由发送分组的源主机指定的传输路径，用来区别由路由器通过路由选择算法确定的路径。源路由主要用于测试某个网络的吞吐量，绕开出错的网络，也可以用于保证分组传输安全的应用中。

(3) 源路由分为严格源路由与松散源路由。

① 严格源路由(SRR)规定分组要经过的路径上的每个路由器，相邻路由器之间不能插入其他路由器，并且经过的路由器顺序不能改变。

② 松散源路由(LRR)规定分组一定要经过的路由器，但不是一条完整的传输路径，中间可以经过其他路由器。

因此，C 对于严格源路由特点的描述是错误的。

答案：C。

5-2-12 分析：设计这道习题的目的是帮助读者加深对 IPv4 分组头选项中"时间戳"项含义与作用的理解。

(1) 时间戳可以记录分组经过每个路由器的本地时间。

(2) 时间戳采用格林尼治时间，单位是毫秒(ms)。

(3) 网络管理员可以利用它追踪路由器的运行状态，分析网络吞吐率、拥塞情况与负荷情况等。

因此，B 的描述是错误的。

答案：B。

5-2-13 分析：

设计本例题的目的是加深读者对于校验和的作用与计算方法的理解。

(1) 大多数 TCP/IP 协议都是采用校验和的方法来进行差错检测。IP 分组头的头校验和的设置是为了保证分组头部的数据完整性。

(2) IP 分组在分组头设置了校验和,而没有对整个分组设置校验,其原因主要有两点。一是 IP 分组头之外的部分属于高层数据,按照高层协议,高层数据都会有相应的校验字段。因此,IP 分组可以不对高层数据进行校验。二是 IP 分组头每经过一个路由器都要改变一次,但数据部分并不改变。在分组头中设置校验和,只对变化部分进行校验是合理的。如果对整个分组进行校验,那么每次都需要对整个分组进行计算,势必要花费路由器大量的时间,使系统性能大大降低。

(3) 计算校验和时首先是将分组头中“校验和”字段值置 0,然后将整个分组头按 16 位进行划分,将各段相加之和取反得校验和。发送分组时,将校验和插入分组头的“校验和”字段中。

解:校验和计算过程如图 5-2 所示。

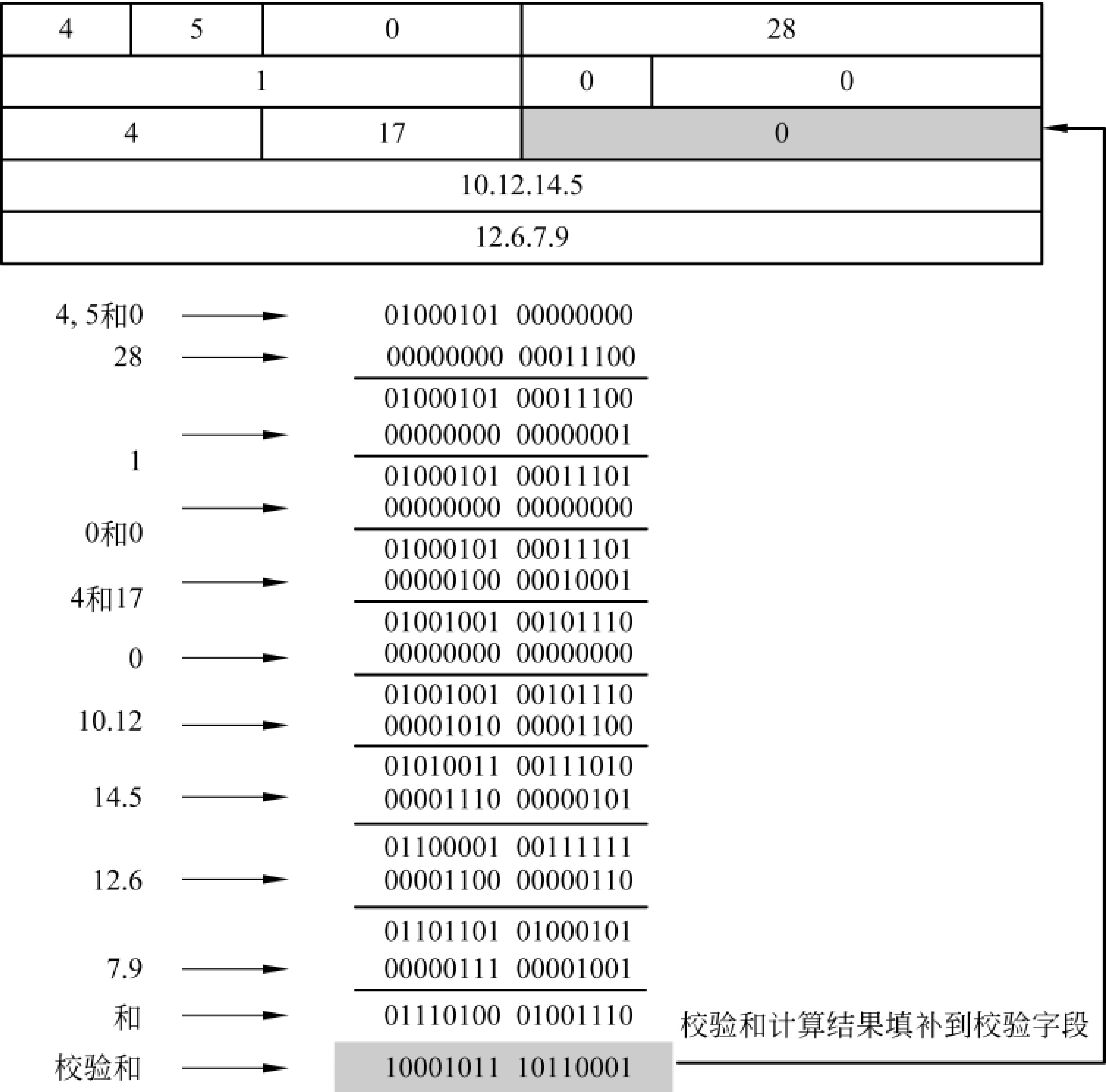


图 5-2 计算校验和过程示意图

这个例子中没有涉及高位溢出的情况。

答案:校验和为 10001011 10110001。

5.3 IPv4 地址

5-3-1 分析:二进制数与十进制数之间不存在简单的 3 位或 4 位的关系,而需要根据

每1位代表的数值进行累加计算。记住表5-1的内容对快速计算IP地址是有益的。

表5-1 二进制与十进制换算表

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

计算：

十进制数值应该等于

$$\begin{aligned}&0\times 2^7+1\times 2^6+1\times 2^5+0\times 2^4+1\times 2^3+1\times 2^2+1\times 2^1+1\times 2^0\\&=0\times 128+1\times 64+1\times 32+0\times 16+1\times 8+1\times 4+1\times 2+1\times 1\\&=64+32+8+4+2+1=111\end{aligned}$$

答案：二进制数001101011可以转换成十进制数111。

5-3-2 分析：一个点分十六进制数代表8位的二进制数。将二进制数转换成点分十六进制数的第一步首先是将二进制数从右向左按8位为一组来划分；如果二进制位数不能够被8整除，则在左边加0；然后再将每一个8位二进制数转换成十进制数。

计算：

(1) 将二进制数从右向左按8位分组

11011110 11100000 00001111 01010101

(2) 将二进制数转换成十进制数

第1个字节 11011110＝128＋64＋16＋8＋4＋2＝222

第2个字节 11100000＝128＋64＋32＝224

第3个字节 00001111＝8＋4＋2＋8＋1＝15

第4个字节 01010101＝64＋16＋4＋1＝85

答案：转换后的点分十六进制数为222.224.15.85。

5-3-3 分析：首先将每1位十六进制数表示为4位二进制数，然后将顺序排列二进制数。十六进制数与二进制数的对应关系如表5-2所示。

表5-2 十六进制数与二进制数的对应关系

十六进制	二进制	十六进制	二进制	十六进制	二进制	十六进制	二进制
0	0000	4	0100	8	1000	C	1100
1	0001	5	0101	9	1001	D	1101
2	0010	6	0110	A	1010	E	1110
3	0011	7	0111	B	1011	F	1111

计算：

十六进制	A	B	A	C	A	B	3	2
二进制数	1010	1011	1010	1100	1010	1011	0011	0010

答案：十六进制ABACAB32转换为二进制数是10101011 10101100 10101011 00110010。

5-3-4 分析：将十进制数转换为二进制数的方法是：重复用2来除十进制数，得到的

余数作为二进制数的数值,从最低位有意义的数位开始排列。

计算:

(1) 十进制数 157 除以 2

157/2=78 余 1

(2) 十进制数 78 除以 2

78/2=39 余 0

(3) 十进制数 39 除以 2

39/2=19 余 1

(4) 十进制数 19 除以 2

19/2=9 余 1

(5) 十进制数 9 除以 2

9/2=4 余 1

(6) 十进制数 4 除以 2

4/2=2 余 0

(7) 十进制数 2 除以 2

2/2=1 余 0

(8) 十进制数 1 除以 2

1/2=0 余 1

答案:十进制数 157 转换成二进制数为 10011101。

5-3-5 分析:这个例题训练的目的是检查读者对 IP 地址最常用的二进制表示法、点分十进制表示法以及相互转换方法的理解。

IP 地址有二进制、点分十进制、十六进制 3 种表示方法,其中常用的是二进制与点分十六进制表示法。图 5-3 给出二进制与点分十六进制 IP 表示法的对应关系。需要注意的是,点分十进制的 IP 地址的每个字节仅有 8 比特,因此每个点分十进制数一定在 0~255。本题可以按照二进制与点分十六进制 IP 地址表示法的对应关系计算,给出答案。

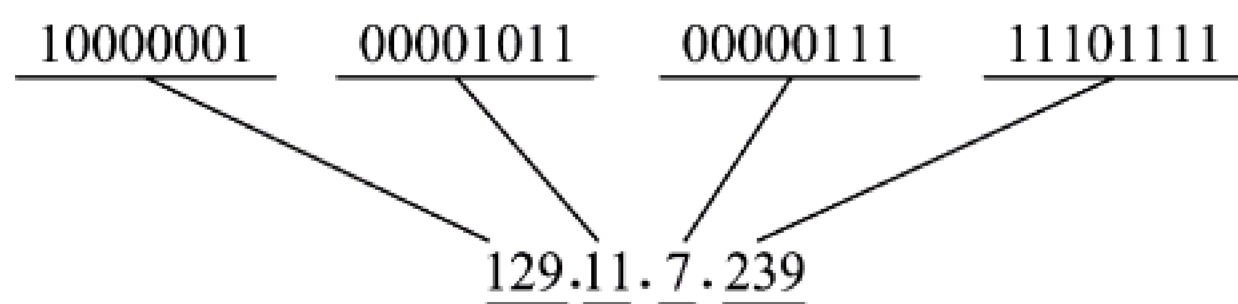


图 5-3 二进制与点分十六进制 IP 地址表示法的对应关系

答案:129.11.7.239。

5-3-6 分析:这个例题用来训练读者将点分十进制的 IP 地址转换成二进制 IP 地址的能力。

解答:224 11100000

115 10011111

25 00011001

255 11111111

答案:11100000 10011111 00011001 11111111

5-3-7 分析:这个例题用以加深读者对 IP 地址分类方法,及 A~E 等各类地址特征的

理解。

（1）IPv4 地址总数

IP 地址长度为 32 位，因此所有的 IP 地址总数为 2^{32} 个。

（2）标准分类地址的特点

① 标准分类的 A 类地址规定 32 位 IP 地址的第 1 位为 0，其他的 31 位可以设置，那么 A 类 IP 地址的数量应该是 2^{31}。

② 标准分类的 B 类地址规定 32 位 IP 地址的第 1、2 位为 10，其他的 30 位可以设置，那么 B 类 IP 地址的数量应该是 2^{30}。

③ 标准分类的 C 类地址规定 32 位 IP 地址的第 1～3 位为 110，其他的 29 位可以设置，那么 C 类 IP 地址的数量应该是 2^{29}。

计算：

各类地址所占的比例数分别为：

① A 类地址所占的比例 $=2^{31}/2^{32}=1/2=50\%$。

② B 类地址所占的比例 $=2^{30}/2^{32}=1/4=25\%$。

③ C 类地址所占的比例 $=2^{29}/2^{32}=1/8=12.5\%$。

答案：A 类地址占 50%；B 类地址占 25%；C 类地址占 12.5%。

5-3-8 分析：这个例题用来检查读者对二进制 IP 地址分类方法的理解。本题可以从标准分类 IP 地址规定的 32 位 IP 地址前 3 位的数值来判断地址类型。

A 类地址的第 1 位为 0；B 类地址的第 1、2 位为 10；C 类地址的第 1～3 位为 110；D 类地址的第 1～4 位为 1110；E 类地址的第 1～4 位为 1111。

答案：

A. 00000001 00001101 00001100 0010000 的第 1 位为 0，为一个 A 类地址。

B. 11010000 10000011 00000011 10000011 的第 1～3 位为 110，为一个 C 类地址。

C. 10100011 10101111 10001110 00011111 的第 1、2 位为 10，为一个 B 类地址。

D. 11110000 10010011 11011001 00001111 的第 1～4 为 1111，为一个 E 类地址。

5-3-9 分析：这个例题用来检查读者对 IP 地址点分十进制表示方法的理解。本题可以从点分十进制的 IP 地址第 1 字节的数值来判断地址类型。

A 类地址的第 1 字节的数值为 0～127；B 类地址的第 1 字节的数值为 128～191；C 类地址的第 1 字节的数值为 192～223；D 类地址的第 1 字节的数值为 224～239；E 类地址的第 1 字节的数值为 240～255。

A. 228.12.33.0 的第 1 位为 228，在 224～239 之间，为一个 D 类地址。

B. 193.1.222.255 的第 1 位为 193，在 192～223 之间，为一个 C 类地址。

C. 12.1.1.1 的第 1 位为 12，在 0～127 之间，为一个 A 类地址。

D. 134.2.220.255 的第 1 位为 134，在 128～191 之间，为一个 B 类地址。

答案：

A. 228.12.33.0 是一个 D 类地址。

B. 193.1.222.255 是一个 C 类地址。

C. 12.1.1.1 是一个 A 类地址。

D. 134.2.220.255 是一个 B 类地址。

5-3-10 分析：设计该例题的目的是检查读者对地址掩码、IP地址结构与网络地址的理解。

标准分类IPv4地址的结构如图5-4所示。标准分类的IP地址是由网络号net ID与主机号host ID两部分组成的。网络号用来标识一个网络；主机号用来标识网络中的一台主机或路由器的连接。



图5-4 IP地址的结构

对应于IPv4地址的分层结构，标准分类的IP地址掩码如图5-5所示。

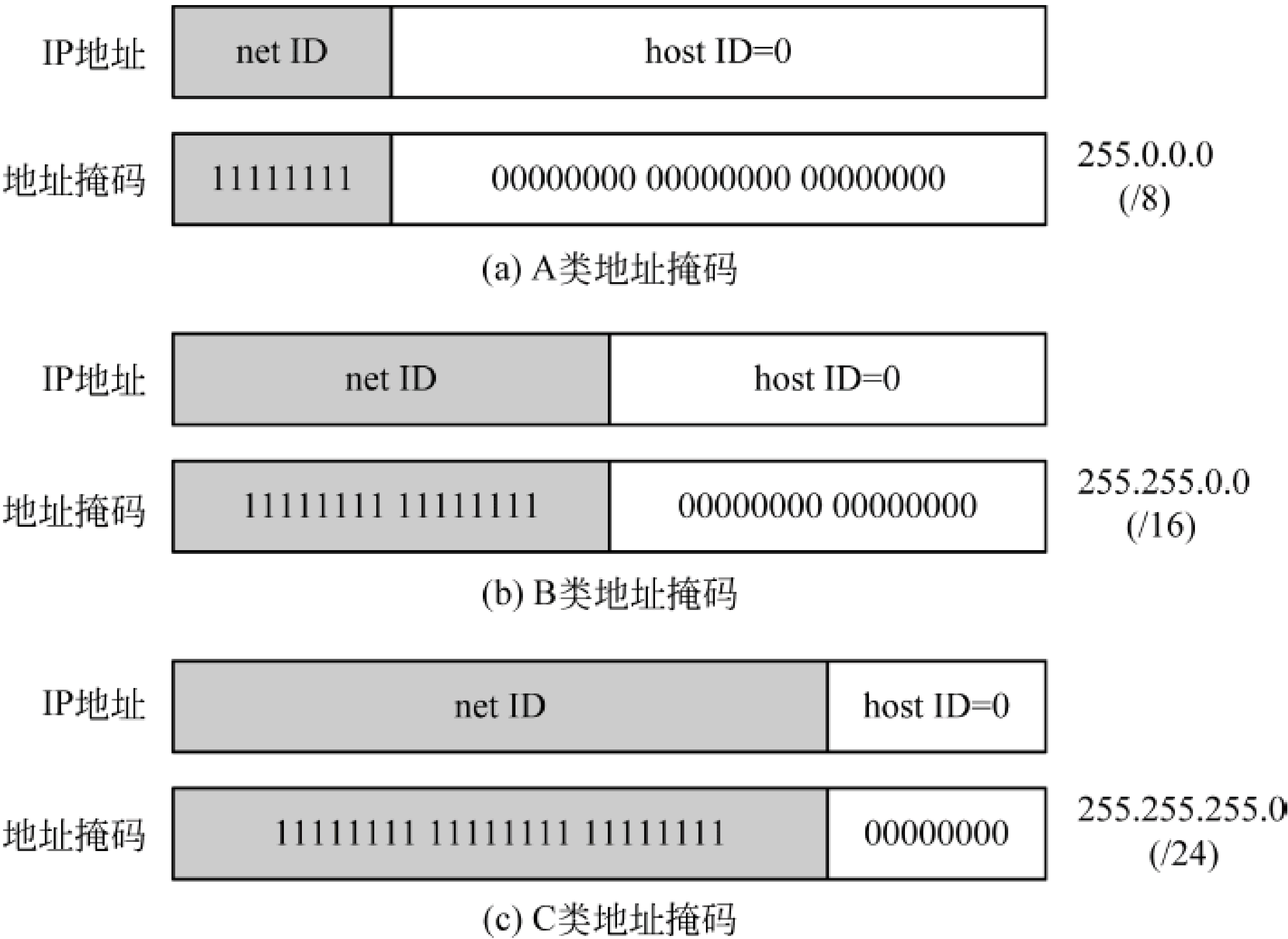


图5-5 标准分类的IP地址掩码

掌握以上的基本知识之后，就可以着手回答问题。完成这道习题，需要分3步来做：

(1) 对标准分类的IP地址类的判断。

(2) 根据对应的IP地址的类，确定对应的地址掩码。

(3) 将IP地址与地址掩码进行“与”操作之后，可以得出对应的网络地址。

计算：

A. 25.1.1.1是一个A类地址；标准分类A类地址的掩码是255.0.0.0，也可以记为/8；那么相应的网络地址为25.0.0.0。

B. 151.1.222.25是一个B类地址；标准分类B类地址的掩码是255.255.0.0，也可以记为/16；那么相应的网络地址为151.1.0.0。

C. 193.2.220.250是一个C类地址；标准分类C类地址的掩码是255.255.255.0，也可以记为/24；那么相应的网络地址为193.2.220.0。

D. 222.12.33.1也是一个C类地址；标准分类C类地址的掩码是255.255.255.0，也可以记为/24；那么相应的网络地址为222.12.33.0。

答案：

A. 25.1.1.1掩码是255.0.0.0(/8)，网络地址为25.0.0.0。

B. 151.1.222.25掩码是255.255.0.0(/16)，网络地址为151.1.0.0。

C. 193.2.220.250 掩码是 255.255.255.0(/24),网络地址为 193.2.220.0。

D. 222.12.33.1 掩码是 255.255.255.0(/24),网络地址为 222.12.33.0。

5-3-11 分析:设计该例题的目的是检查读者对各类 IP 地址知识的全面掌握情况。解决这个问题需要掌握以下知识。

(1) 标准分类的 IP 地址包括 3 种基本类型:公用 IP 地址、专用 IP 地址与特殊 IP 地址。

(2) 公用 IP 地址是指可以在 Internet 网中作为目的 IP 地址与源 IP 地址,路由器可以根据这些 IP 地址进行路由选择处理,如 12.2.1.10 是 A 类 IP 地址、191.1.2.3 是 B 类 IP 地址、222.12.5.1 是 C 类 IP 地址。

(3) 标准分类的 IP 地址中保留了一部分作为专用 IP 地址。专用 IP 地址如表 5-3 所示。

表 5-3 专用 IP 地址

类	net ID	块 数
A	10.0.0	1
B	172.16～172.31	16
C	192.168.0～192.168.255	255

专用 IP 地址只能用于内部网络中,不能在 Internet 中作为目的地址与源地址使用。Internet 中的路由器不转发使用专用 IP 地址的分组。如果 IP 地址为 10.0.0.12,或者是 172.15.1.1、192.168.2.1,都属于专用 IP 地址,无论是作为目的地址或源地址,路由器都不会处理和转发该分组。

(4) 特殊 IP 地址。

特殊 IP 地址分为直接广播(directed broadcasting)地址、受限广播(limited broadcasting)地址、这个网络上的特定主机地址与回送地址(lookback address)。

① 直接广播地址:在 A 类、B 类与 C 类 IP 地址中,如果主机号 host ID 为全 1,那么这个地址为直接广播地址。它是用来使路由器将一个分组以广播方式发送给特定网络上的所有主机。直接广播地址只能作为分组中的目的地址。

② 受限广播地址:如果网络号与主机号的 32 位全 1 的 IP 地址(255.255.255.255)为受限广播地址。它是用来将一个分组以广播方式发送给本网络内部的所有主机。

③ 这个网络上的特定主机地址:IP 地址的网络号为全 0,主机号为确定的值,这样的分组被限制在本网内部,由特定的主机号对应的主机接收该分组。

④ 回送地址:A 类 IP 地址中 127.0.0.0 是回送地址。回送地址用于网络软件测试和本地进程间通信。无论什么程序,一旦使用回送地址作为目的地址来发送数据,那么协议软件不会将数据传送到网络上,并立即将它回送。

根据以上知识,可以作出以下的判断:

A. 221.1.25.255 符合直接广播地址的特征。这是一个典型的 C 类 IP 地址,网络地址为 221.1.25.0,其主机号为 255(11111111)。如果一个分组的目的地址为 221.1.25.255,那么路由器将该分组发送到网络地址为 221.1.25.0 的网络的所有主机。

B. 255.255.255.255 符合受限广播地址的特征。如果一个分组的目的地址为 255.255.255.255,那么路由器不将该分组转发到外部网络,而直接以广播方式将该分组发送本网络内部的所有主机。

C. 0.0.0.102 符合受限这个网络上的特定主机地址的特征。如果一个分组的目的地址为 0.0.0.10,那么路由器不将该分组转发到外部网络,而直接以广播方式将该分组发送到本网络内部的主机号为 102 的主机。

D. 70.0.0.0 为 net ID=70 的一个 A 类网络的网络地址,不是特殊 IP 地址。

E. 127.1.2.3 符合回送地址的特征。如果一个分组的目的地址为 127.1.2.3,那么该分组在发送到网络之前就被回送到测试程序。

F. 10.1.2.3 符合于 A 类专用 IP 地址(10.0.0.0)的特征,属于专用 IP 地址。

答案:

A. 221.1.25.255 属于直接广播地址。

B. 255.255.255.255 属于受限广播地址。

C. 0.0.0.102 属于受限这个网络上的特定主机地址。

D. 70.0.0.0 为 net ID=70 的一个 A 类网络的网络地址,不是特殊 IP 地址。

E. 127.1.2.3 属于回送地址。

F. 10.1.2.3 属于专用 IP 地址。

5-3-12 分析:设计该例题的目的是为了帮助读者理解"受限广播地址""直接广播地址"与"这个网络特定主机地址"之间的区别。

(1) 主机 A 发送一个目的地址为受限广播地址的"255.255.255.255"IP 分组。受限广播地址的特点是:这个分组只能以广播方式发送给本网络的所有主机,路由器不向外转发该分组。因此,只有主机 B、主机 C 能够收到该分组。交换机工作在 MAC 层,对 IP 分组的转发没有影响。

(2) 主机 A 发送一个目的地址为直接广播地址 191.2.255.255 的 IP 分组。直接广播地址的特点是:路由器将转发该分组到 191.2.0.0 的子网所有的主机。因此,主机 D、主机 E 能够接收到该分组。

(3) 主机 A 发送一个目的地址为"这个网络特定主机地址"0.0.12.10 的 IP 分组。直接广播地址的特点是:网络地址部分为全 0,路由器不转发,而是直接发给本网络中地址为 12.10 的主机。因此,主机 B 可以接收到这个分组。

5-3-13 分析:B 类地址的主机号 host ID 为全 1,那么这个地址为直接广播地址,它是通过路由器将一个分组以广播方式发送给自己所在子网的所有主机。

子网掩码为 255.255.252.0,即前缀长度为/22。这样主机的 IP 地址的前 2 个字段 191.1 不受影响,最后一个字段直接可以看出是 255。那么,需要考虑的就是地址的第 3 个字段 77。

77 对应的二进制数为:	01001101
掩码的第 3 个字段的二进制数为:	11111100
相与之后:	01001100
主机号取全 1:	01001111

第 3 个字段用十进制表示为 79。

主机的 IP 地址为 191.1.77.55/22 的广播地址为 191.1.79.255。

因此,D 的描述是正确的。

答案:D。

5-3-14 分析:设计该例题的目的是检查读者对标准 IP 地址分类方法、地址块中网络地址、广播地址的表示方法,以及可用于分配给主机的 IP 地址等综合知识的掌握情况。

解决这个问题可以采用以下的步骤:

(1) 根据标准 IP 地址分类方法,判断该地址块的地址类型。

(2) 根据地址类型与对应的掩码,确定网络地址。

(3) 取主机号为全 1 的地址为广播地址。

(4) 地址块中除去网络地址与广播地址,其余的部分都可以分配给主机。根据该原则确定可以分配给主机的 IP 地址范围。

基于以上分析,可以作出判断:

(1) 由于没有进行子网划分,属于标准分类的网络地址。点分十进制的 IP 地址的第一个字节数为 169,因此属于标准的 B 类 IP 地址。标准的 B 类 IP 地址的掩码为 255.255.0.0(/16),因此该地址块的网络地址为 169.1.0.0。

(2) 该地址块的主机号 host ID 长度为 16 位,host ID 的 16 位全 1 为广播地址,即 169.1.255.255。

(3) 该地址块的 IP 地址范围:169.1.0.0~169.1.255.255。其中,第一个 IP 地址 169.1.0.0 为网络地址,最后一个 IP 地址是 169.1.255.255 是广播地址,这两个地址不能够分配做主机 IP 地址。因此,可以分配给主机的第一个地址应该比 169.1.0.0 大 1,即 169.1.0.1;最后一个可以分配给主机的 IP 地址应该比广播地址 169.1.255.255 小 1,即 169.1.255.254。

可分配给主机的 IP 地址范围是:169.1.0.1~169.1.255.254。

答案:

(1) 掩码为 255.255.0.0(/16),地址块的网络地址为 169.1.0.0。

(2) 广播地址为 169.1.255.255。

(3) 可分配给主机的 IP 地址范围是:169.1.0.1~169.1.255.254。

5-3-15 分析:设计该习题的目的是检查读者对于子网划分、子网掩码与子网地址知识的理解与掌握的程度。解决这个问题需要具备以下基础知识:

(1) 划分子网后的 IP 地址为 3 层结构,即:net ID-subnet ID-host ID。同一子网中的所有主机必须使用相同的子网号 subnet ID。

(2) 根据 IP 地址和子网掩码“与”运算的结果来判断子网号 subnet ID 的值。

计算:

(1) 将点分十进制地址 191.230.34.56 转换为二进制形式:

10111111　11100110　00100010　00111000

(2) 将子网掩码 255.255.240.0 转换为二进制形式:

11111111　11111111　11110000　00000000

(3) 将地址与掩码进行"与"运算:

10111111　11100110　00100010　00111000
11111111　11111111　11110000　00000000
10111111　11100110　**0010**0000　00000000

(4) 与运算的结果为:

10111111　11100110　**0010**0000　00000000

subnet ID 为:00100000 或 32

答案:subnet ID 为:00100000 或 32。

5-3-16　分析:设计这个例题的目的是让读者用快捷方法计算子网地址,进一步加深对子网划分与子网地址计算的理解。如果子网掩码是连续的,可以用一种快捷的方法来处理。

以这题为例,子网掩码是 255.255.240.0,也就是说,前 2 字节是全 1,那么在目的地址与掩码进行"与"运算时,目的地址的前 2 字节的值肯定是不会改变的,即先确定 191.230 的值,它是一个 B 类 IP 地址,其中前 16bit 是 netID,只需要对第 3 字节进行计算。快捷方法的规律是:

(1) 如果子网掩码是 255 时,就复制这个字节的值到地址中。

(2) 如果子网掩码是 0 时,就在地址中用 0 代替这个字节。

(3) 如果子网掩码既不是 255 也不是 0 时,需要将目的地址与掩码转换成二进制,然后根据"与"运算的结果来确定子网地址。

按照上一题给出的计算方法,子网掩码的前 2 字节是 255,因此 IP 地址的前 2 字节 129.240 将复制到子网地址的前 2 字节;子网掩码的第 4 字节为 0,那么子网地址的第 4 字节必然为 0;只需要对 IP 地址与子网掩码的第 3 字节进行"与"运算;其过程如图 5-6 所示。

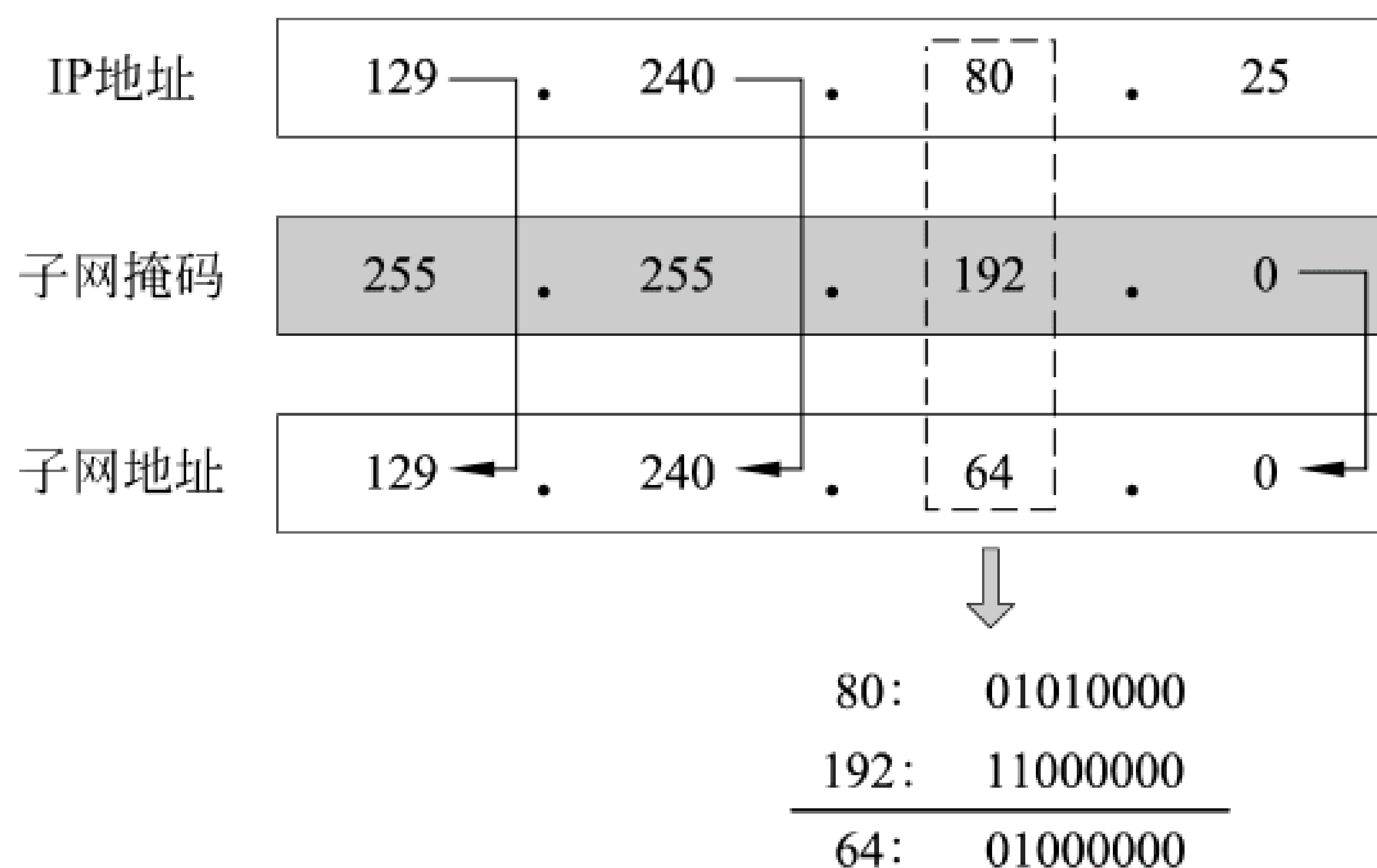


图 5-6　快捷方法计算出子网地址的示例

答案:网络地址为 129.240.64.0。

5-3-17　分析:设计这道题的目的是帮助读者复习求解子网网络地址的方法。

其实这个问题很简单,但是初学者常常被这种提法搞糊涂。主机的 IP 地址与子网掩码相"与"的结果是得出子网的网络地址。同一子网中两台主机的 IP 地址与子网掩码相"与"的结果自然是得出这个子网的网络地址,所以它们一定是相同的。因此,C 的描述是正确的。

答案：C。

5-3-18 分析：设计这道题的目的是帮助读者复习 IP 地址、特殊 IP 地址以及有关规定。

A. 25.1.1.255 是一个正常的 A 类 IP 地址，可以分配给主机。

B. 128.15.2.0 是一个 B 类的 IP 地址，但是最后 8 位为全 0(0)，这是错误的，因此不能分配给主机。

C. 193.2.220.256 是一个 C 类的 IP 地址，但是最后 8 位为全 1(256)，这是错误的，因此不能分配给主机。

D. 127.0.0.0 是保留的回送地址，用于网络软件测试，因此不能分配给主机。

答案：A。

5-3-19 分析：设计这道题的目的是为了加深读者对子网掩码、主机地址长度与主机数的理解。

一个 B 类地址的网络地址长度为 16 位，掩码是 255.255.240.0，表示子网地址 4 位，主机地址长度为剩余的 12 位。

那么，每个网络内部的主机数量等于 $2^{12}-2=4094$（主机地址全 0、与全 1 不能分配）。

因此，B 的值是正确的。

答案：B。

5-3-20 分析：设计这道题的目的是帮助读者进一步理解网络前缀与网络地址的关系。

对于地址 129.120.200.0/21，第 1、2 个字段长度为 16 位，前缀长度是 21 位，因此它只会影响到地址的第 3 个字段。在计算网络地址时，只需要看地址的第 3 个字段 200 的前 5 位的值。

用二进制数表示 200，得 1100 1000。它的前 5 位是 11001，简单地分析，可将 129.120.200.0/21 的网络地址表示为 129.120.1100 1000.0000 0000。

那么，这个子网的 IP 地址应该是在主机号全 0 到主机号全 1 之间：

129.120.1100 1000.0000 0000～129.120.1100 1111.1111 1111

用点分十进制表示，子网的 IP 地址应该是：

129.120.200.0～129.120.207.255

因此，答案给出的 4 个选项中：

A. 129.119.128.1　　B. 129.119.128.254

C. 129.120.207.254　　D. 129.120.208.1

只有 C 在该子网地址的范围内。

答案：C。

5-3-21 分析：设计这道题的目的是加深读者对同属一个子网概念的理解。

实际上，判断两个 IP 地址是不是属于一个子网，就需要计算出对应的子网地址，根据子网地址相同与不同来判断。

B 类地址，子网前缀/20，说明：网络号为 16 位，子网号 4 位。如果都是 B 类地址，那就看子网地址是否相同。

(1) 判断 A. 180.81.16.254/20 与 180.81.32.254/20。

180.81.16.254/20 的第 3 字段值为 16，对应二进制数是 0001 0000，子网地址：0001；

180.81.32.254/20 的第 3 字段值为 32，对应二进制数是 0010 0000，子网地址：0010；

这两个子网地址号不同,不属于一个子网。

(2) 判断 B. 180.81.16.254/20 与 180.81.17.1/20。

180.81.16.254/20 的第 3 字段值为 16,对应二进制数是0001 0000,子网地址:0001;

180.81.17.1/20 的第 3 字段值为 16,对应二进制数是0001 0001,子网地址:0001;

这两个子网地址号相同,属于一个子网。

(3) 判断 C. 180.81.16.254/20 与 180.81.33.1/20。

180.81.16.254/20 的第 3 字段值为 16,对应的二进制数是0001 0000,子网地址:0001;

180.81.33.1/20 的第 3 字段值为 33,对应的二进制数是0010 0001,子网地址:0010;

这两个子网地址号不同,不属于一个子网。

(4) 判断 D. 180.81.17.254/20 与 180.81.32.254/20。

180.81.17.254/20 的第 3 字段值为 17,对应的二进制数是0001 0001,子网地址:0001;

180.81.32.1/20 的第 3 字段值为 33,对应的二进制数是0010 0001,子网地址:0010;

这两个子网地址号不同,不属于一个子网。

答案:B。

5-3-22 分析:设计这道习题的目的是加深读者对主机直接通信条件的理解。只有主机的网络地址处于一个子网中,就可以不需要通过路由器转发而直接通信。网络地址不同,表明它们不在一个子网中,它们之间的通信需要通过路由器转发。

求解:

(1) 4 台主机中哪些可以直接通信?哪些需要通过路由器才可以通信?

子网掩码为 255.255.255.224,即前缀为/27。

主机 A:210.20.1.112 网络地址:210.20.1.96

主机 B:210.20.1.120 网络地址:210.20.1.96

主机 C:210.20.1.135 网络地址:210.20.1.128

主机 D:210.20.1.202 网络地址:210.20.1.192

因此,主机 A、B 在一个子网中,可以直接通信。主机 A、B 与主机 C 或主机 D,以及主机 C 与主机 D 之间不能直接通信,要通过路由器转发。

(2) 增加的主机 E 要与主机 D 直接通信,主机 E 的 IP 地址应该在哪个范围内?

实际上就是要知道主机 D 所在子网的地址空间。

210.20.1.202/27,网络地址:210.20.00000001.11001010

该子网的 IP 地址空间:201.20.1.192～201.20.1.222。

主机 E 的 IP 地址范围:201.20.1.192～201.20.1.222(不包括 210.20.1.202)。

(3) 如果要使 4 台主机都能够直接通信,需要对网络地址做什么样的调整?

实际上是要将 4 个 IP 地址聚合。汇聚后的掩码作为主机的共同掩码即可。汇聚时只用看第 4 个字段:

210.20.1.96 第 4 个字段:0110 0000

210.20.1.96 第 4 个字段:0110 0000

210.20.1.128 第 4 个字段:1000 0100

210.20.1.202 第 4 个字段:1100 1010

汇聚以后的前缀只能取/24,即可实现 4 个地址在同一子网内,子网的网络地址是 210.

20.1.0/24,或主机的掩码是255.255.255.0,这样它们之间可以直接通信。

答案:

(1) 主机A、B在一个子网中,可以直接通信。主机A、B与主机C或主机D,以及主机C与主机D之间不能直接通信,要通过路由器转发。

(2) 主机E的IP地址范围:201.20.1.192~201.20.1.222(不包括210.20.1.202)。

(3) 掩码为255.255.255.0,4台主机之间可以直接通信。

5-3-23 分析:设计这道习题的目的是帮助读者理解子网掩码的设计方法。

子网掩码的选择需要考虑两个因素:满足子网数的要求,满足主机数的要求。

本题要求的子网数为5,那么意味着子网号长度至少为3位;因为子网号长度至少为2位,只能分配给4个子网。子网号长度至少为3,可以容纳8个子网。

要求接入的主机数至少为20台,那么主机号至少为5位,这样可以分配的主机号为32。

如果用户希望将网络划分为5个子网,每一个子网最多接入20台主机,那么4组掩码中最适合的是C。

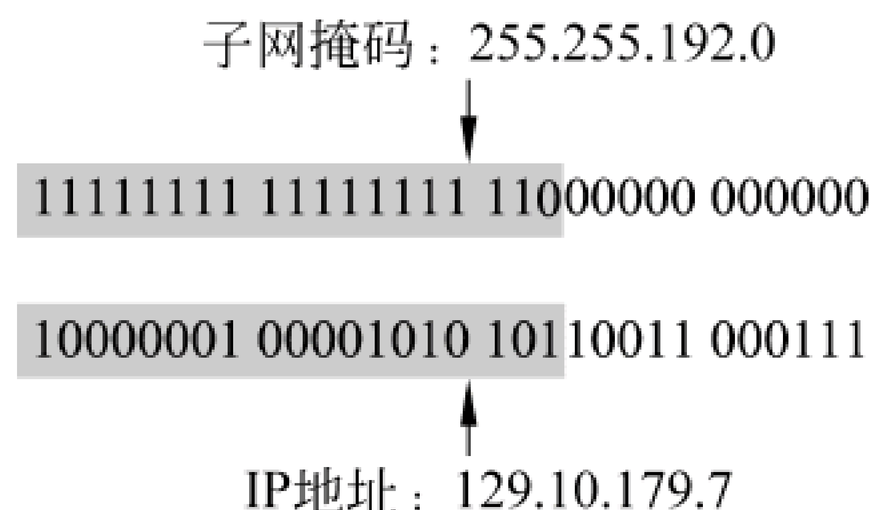
答案:C。

5-3-24 分析:设计该例题的目的是检查读者对标准IP地址分类方法、地址块中网络地址、广播地址的表示方法,以及可用于分配给主机的IP地址等综合知识的掌握情况。

解决这个问题可以采用以下的步骤:

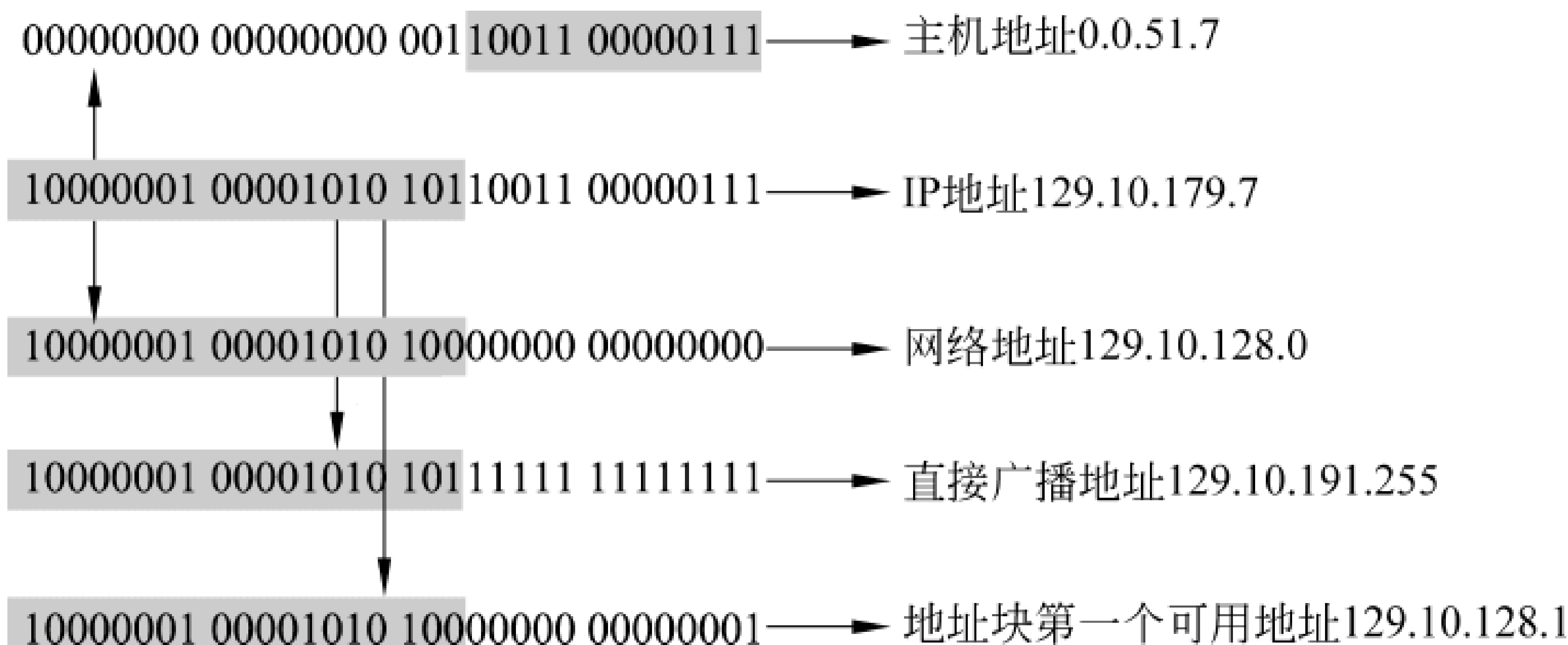
(1) IP地址的类型很容易判断,129.10.179.7从点分十六进制的第一个129就可以看出是一个B类IP地址。如果从二进制的IP地址的前两位10也可以看出是一个B类地址。

(2) 比较IP地址与子网掩码,找出网络号与子网号。这个过程为:



可以看出,B类IP地址前16位是网络号,子网号用了2位,主机号有14位。

(3) 知道了IP地址的结构,找出网络地址、直接广播地址、主机号以及子网中第一个可用IP地址也就很容易了,其过程为:



答案:

【1】B类IP地址

【2】129.10.128.0

【3】129.10.191.255

【4】0.0.51.7

【5】129.10.128.1

5-3-25 分析：上一个问题是给出子网掩码之后，计算子网的数量，并计算各个子网的地址范围。这道题是要求读者根据给定的条件，设计一个符合要求的子网地址结构。实际上是要求读者自己决定应该使用怎样的子网掩码。子网地址设计的原则与上一题相同。

(1) 181.55.0.0是一个典型的B类IP地址，默认掩码为255.255.0.0(或/16)。

(2) 需要划分1000个子网，加上子网地址与子网受限广播地址，实际上需要划分出1002个子网。划分子网地址的实质是要借用B类IP地址中的16位主机号host ID的高n位作为子网号subnet ID。因此，问题的关键是选择什么样的n值，使它可以标识出1002个子网。$2^{10}=1024$，如果选择$n=10$，可以满足本题的要求。符合本题条件的3层IP地址结构如图5-7所示。子网掩码为：255.255.255.192(或/26)。

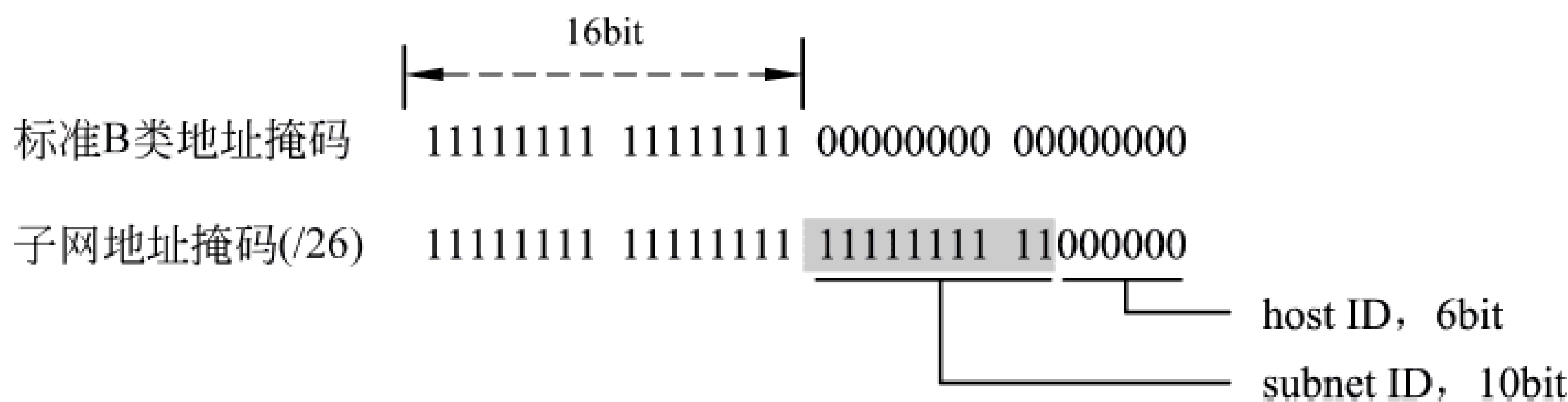


图5-7　符合本题条件的3层IP地址结构

(3) 确定1024个子网地址的覆盖范围。

① 第1个子网地址：

第1个子网地址的subnet ID取全0，第3字节二进制值为00000000，第4字节值为00000000，因此第1个子网地址的最小地址为181.55.0.0。

第1个子网地址的subnet ID取全0仍不变，最大的地址的host ID值为全1，这样第4字节的二进制值为00111111，点分十进制值为63，因此第1个子网地址的最大地址为181.55.0.63。

第1个子网地址的最小地址为181.55.0.0，最大地址为181.55.0.63。

第1个子网IP地址的覆盖范围为181.55.0.0～181.55.0.63。

② 第2个子网地址：

第2个子网地址的subnet ID取1，第3字节二进制值为00000000，第4字节值为01000000，因此第1个子网地址的最小地址为181.55.0.64。

第2个子网地址的subnet ID取1仍不变，最大地址的host ID值为全1，这样第4字节的二进制值为01111111，点分十进制值为127，因此第1个子网地址的最大地址为181.55.0.127。

第2个子网地址的最小地址为181.55.0.64，最大地址为181.55.0.127。

第2个子网IP地址的覆盖范围为181.55.0.64～181.55.0.127。

③ 第1024个子网地址：

第 1024 个子网地址的 subnet ID 取全 1,第 3 字节二进制值为 11111111,第 4 字节值为 11000000,因此第 1 个子网地址的最小地址为 181.55.255.192。

第 1024 个子网地址的 subnet ID 取全 1 仍不变,最大地址的 host ID 值为全 1,这样第 4 字节的二进制值为 11111111,点分十进制值为 255,因此第 1024 个子网地址的最大地址为 181.55.0.63。

第 1024 个子网地址的最小地址为 181.55.255.192,最大地址为 181.55.255.255。

第 1024 个子网 IP 地址的覆盖范围为 181.55.255.192～181.55.255.255。

答案:

(1) 选择子网掩码为:255.255.255.192(或/26),即子网号为 10 位,可以将 B 类 IP 地址 181.55.0.0 划分出 1024 个子网,子网掩码为 255.255.0.0(或/16)。

(2) 1024 个子网地址的覆盖范围为:

第 1 个子网 IP 地址　　181.55.0.0～181.55.0.63

第 2 个子网 IP 地址　　181.55.0.64～181.55.0.127

……

第 1024 个子网 IP 地址　　181.55.255.192～181.55.255.255

(3) 除去网络地址、广播地址,以及每个子网的子网地址、广播地址,可以分配给主机的 IP 地址如图 5-8 中虚线部分所示。

第1个子网IP地址	181.56.0.0	181.56.0.0	…	181.56.0.63	181.56.0.63
第2个子网IP地址	181.56.0.64	181.56.0.65	…	181.56.0.126	181.56.0.127
第3个子网IP地址	181.56.0.128	181.56.0.129	…	181.56.0.190	181.56.0.191
第4个子网IP地址	181.56.0.192	181.56.0.193	…	181.56.0.190	181.56.0.255
			…		
第1023个子网IP地址	181.56.255.128	181.56.255.129	…	181.56.255.190	181.56.255.191
第1024个子网IP地址	181.56.255.192	181.56.255.193	…	181.56.255.254	181.56.255.255

图 5-8　可以分配给主机的 IP 地址

可分配给主机的 IP 地址的子网共有 1022 个;每个子网可以分配给主机的 IP 地址共有 $2^5-2=62$ 个。

(4) 对于一个规模较大的子网地址的规划过程,有两种基本的方法。第一种方法是从地址小的子网地址开始计算,其过程如图 5-9 所示。从图 5-9 中可以看出,第 1 个子网地址是从 181.55.0.0～181.55.0.63,IP 地址数量为 64;这个数值可以根据子网地址结构计算出来。那么,第 2 个子网的起始地址 181.55.0.64 是在第 1 个子网广播地址 181.55.0.63 加 1。这个规律可以保持到最后一个子网地址的推算过程。第二种方法是从地址最大的子网地址开始计算。第 1024 个子网地址是从 181.55.255.192 到 181.55.255.255,IP 地址数量为 64;这个数值可以根据子网地址结构计算出来。那么,第 1023 个子网的最大地址 181.55.255.191 等于第 1024 个子网广播地址 181.55.255.192 减 1。

需要注意的是,以上讨论的是子网地址等长的规划。

5-3-26　分析:设计本题的目的是要考察读者对可变长度子网掩码 VLSM 地址规划方

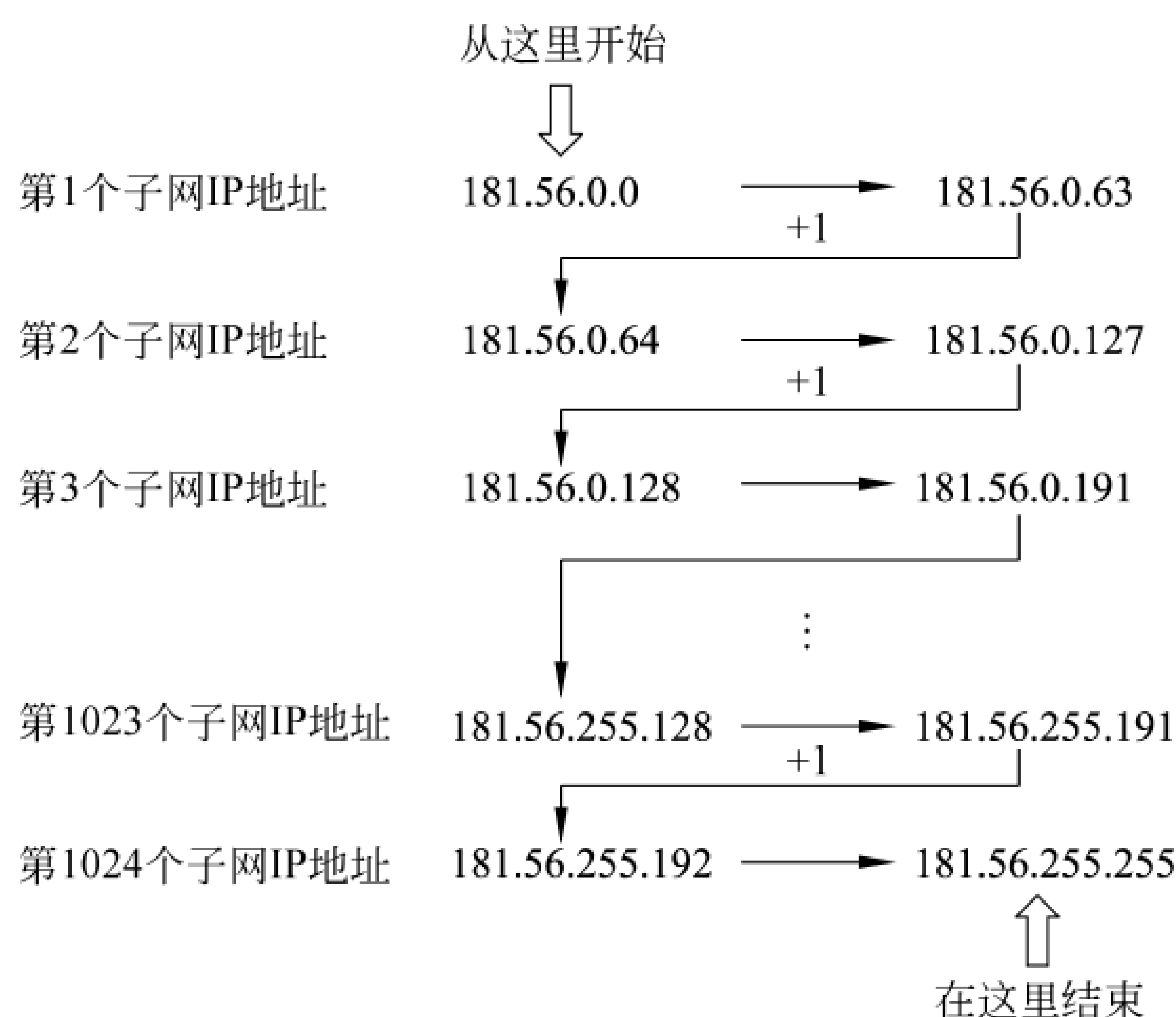


图 5-9　从地址小的子网地址开始计算的过程示意图

法掌握的情况。IP 协议允许使用变长子网的划分。本例题是将一个 C 类 IP 地址分为 3 个部分,其中子网 1 的地址空间是子网 2 与子网 3 的地址空间的两倍。

(1) 计算子网 1 的地址空间。

首先可以使用子网掩码为 255.255.255.128,将一个 C 类 IP 地址划分为两半。在二进制计算中,运算过程是:

主机的IP地址:	11001010 00111100 00011111 00000000	(202.60.31.0)
子网掩码:	11111111 11111111 11111111 10000000	(255.255.255.128)
与运算结果:	11001010 00111100 00011111 00000000	(202.60.31.0)

运算结果表明:可以将 202.60.31.1～202.60.31.126 作为子网 1 的 IP 地址,而将余下的部分进一步划分为两半。由于 202.60.31.127 第 4 个字节是全 1,被保留作为广播地址,不能使用;子网 1 与子网 2、子网 3 的地址空间交界点在 202.60.31.128;可以使用子网掩码为 255.255.255.192。

(2) 计算子网 2 与子网 3 的地址空间。

子网 2 与子网 3 的地址空间的计算过程为:

主机的IP地址:	11001010 00111100 00011111 10000000	(202.60.31.128)
子网掩码:	11111111 11111111 11111111 11000000	(255.255.255.192)
与运算结果:	11001010 00111100 00011111 10000000	(202.60.31.128)

将平分后的两个较小的地址空间分配给子网 2 与子网 3。对于子网 2 来说,第一个可用的地址是 202.60.31.129,最后一个可用的地址是 202.60.31.190。子网 2 的第一个可用的地址是 202.60.31.129 到 202.60.31.190。

下一个地址 202.60.31.191 中 191 是全 1 的地址,需要留做广播地址。接下来的一个

地址是 202.60.31.192,它是子网 3 的第一个地址。那么,子网 3 的 IP 地址应该是从 202.60.31.193 到 202.60.31.254。

答案:确定 3 个子网 IP 地址空间。

采用变长子网的划分的三个子网的 IP 地址分别为:

(1) 子网 1 地址空间为　202.60.31.1~202.60.31.126

子网掩码为　255.255.255.128(或/25)

(2) 子网 2 地址空间为　202.60.31.129~202.60.31.190

子网掩码为　255.255.255.192(或/26)

(3) 子网 3 地址空间为　202.60.31.193~202.60.31.254

子网掩码为　255.255.255.192(或/26)

子网 1 允许使用的主机号为 126 个;子网 2 与子网 3 可以使用的主机号均为 61 个。

5-3-27　分析:设计这个例题有两个目的:一是加深读者对于路由汇聚概念与计算方法的理解,二是从地址汇聚的角度去认识城域网 3 层结构的特点。汇聚是用一条路由描述多个网络的一种路由技术,它体现出路由器在选择输出路径时采用的“最长前缀匹配”的原则,是学习网络技术必须掌握的基本知识与技能之一。

计算:

(1) 如果读者已掌握地址汇聚的基本计算方法与规律,对于 152.20.0.0/24、152.20.1.0/24、152.20.2.0/24、152.20.3.0/24,很容易看出,这 4 个地址的前 2 字节相同,第 3 字节不同,寻找最长前缀匹配的过程如图 5-10 所示。

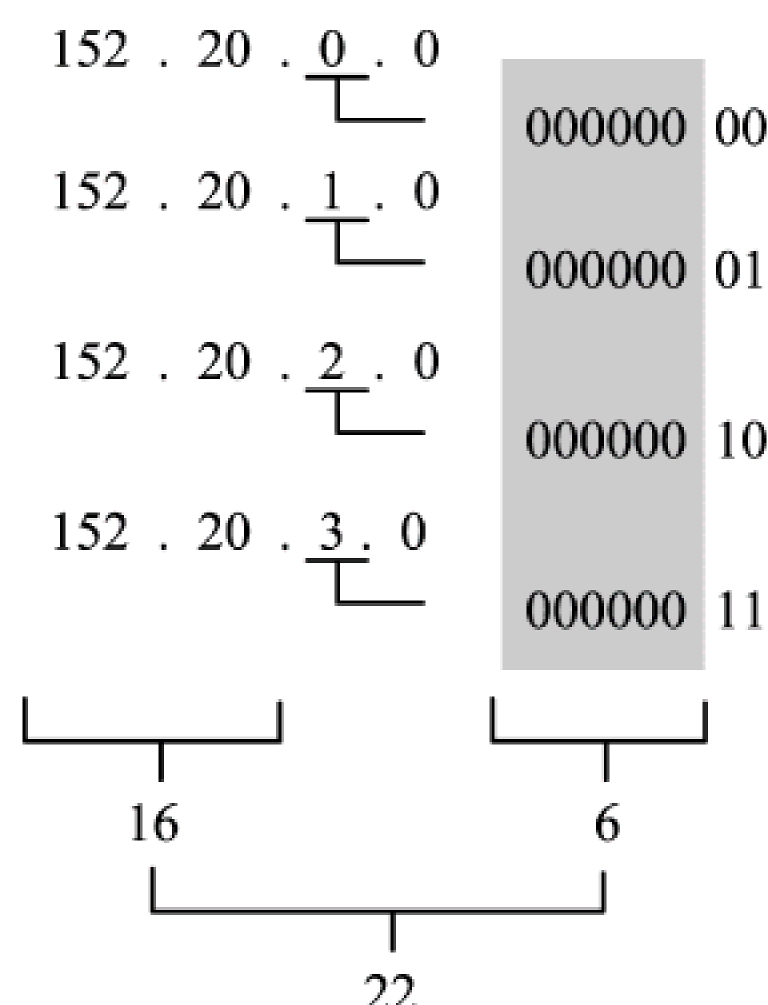


图 5-10　寻找最长前缀匹配的过程示意图

那么,它们共同的前缀只有 22 位,因此位置①汇聚的网络地址为 152.20.0.0/22。

以下问题的解决办法是相同的。

(2) 对于 152.20.4.0/24,152.20.5.0/24,152.20.5.0/24,152.20.7.0/24 这 4 个地址,它们共同的前缀也只有 22 位,因此位置②汇聚的网络地址为 152.20.4.0/22。

(3) 152.20.0.0/22 与 152.20.4.0/22 进一步汇聚后位置⑤的网络地址为 152.20.0.0/21。

(4) 201.120.0.0/24~201.120.7.0/24 共同的前缀只有 21 位,因此位置③汇聚的网络地址为 201.120.0.0/21。

(5) 201.120.8.0/24~201.120.15.0/24 共同的前缀也只有 21 位,因此位置④汇聚的网络地址为 201.120.8.0/21。

(6) 201.120.0.0/21 与 201.120.8.0/21 进一步汇聚后位置⑥的网络地址为 201.120.0.0/20。

答案:

位置①汇聚后的网络地址为 152.20.0.0/22。

位置②汇聚后的网络地址为 152.20.4.0/22。

位置③汇聚后的网络地址为 201.120.0.0/21。

位置④汇聚后的网络地址为 201.120.8.0/21。

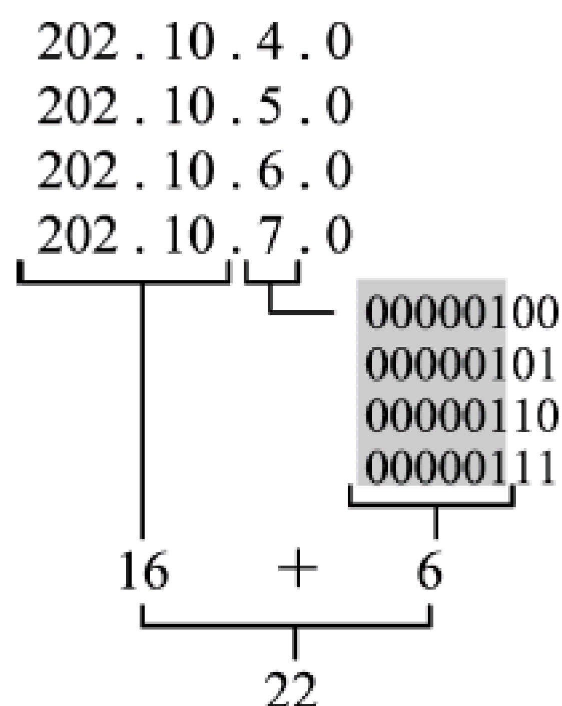
位置⑤汇聚后的网络地址为 152.20.0.0/21。

位置⑥汇聚后的网络地址为 201.120.0.0/20。

5-3-28 分析：设计这个例题的目的是检查读者对于地址汇聚概念的理解。在深入研究路由器工作原理、路由表形成之前，有必要做一些关于地址汇聚的题目，这对于理解路由汇聚与路由表的形成是有益的。计算汇聚后的网络地址就是寻找多个 IP 地址中相同地址位数的过程。

在以上 4 个 IP 地址中，前 2 字节是相同的，读者只需要将第 3 字节转换成二进制数，然后通过比较 4 个 IP 地址中第 3 字节，找出相同的位数即可得出汇聚后的网络地址。

地址汇聚计算的过程为



答案：汇聚后的网络地址为 202.10.4.0/22。

5-3-29 分析：设计这道习题的目的是帮助读者加深理解默认路由的概念。

(1) 已知：一台主机 IP 地址为 11.1.1.100，子网掩码为 255.0.0.0。用户需要给主机配置一个默认路由。

(2) 与主机直接连接的路由器有 4 个 IP 地址与掩码：

Ⅰ. 11.1.1.1，255.0.0.0　　Ⅱ. 11.1.2.1，255.0.0.0

Ⅲ. 12.1.1.1，255.0.0.0　　Ⅳ. 13.1.2.1，255.0.0.0

(3) 选项中只有 A 中Ⅰ."11.1.1.1，255.0.0.0"与Ⅱ."11.1.2.1，255.0.0. 0"的网络地址是 11.0.0.0，与主机的 IP 地址"11.1.1.100，255.0.0.0"的网络地址"11.0.0.0"，在一个 A 类网络中，其他组合的网络地址都不相同。在这种情况下，选项 A 是对的。

答案：A。

5-3-30 分析：设计这道习题的目的是帮助读者加深对地址聚合方法的理解。

(1) 对 4 条路由进行聚合。

由于给出的前缀都是 24，4 个待聚合的地址前 2 个字段值相同，因此只需要对第 3 个字段值进行计算。

191.18.129.0/24	129	1000 0001
191.18.130.0/24	130	1000 0010
191.18.132.0/24	132	1000 0100
191.18.133.0/24	133	1000 0101
聚合地址共同部分是	128	1000 0000

4 个聚合地址中前 5 位相同，那么聚合后的地址前缀为 21。

聚合的地址为：191.18.128.0/21。

（2）挑选答案。

从可供选择的4个地址中可以看出，A是正确的。

答案：A。

5-3-31 分析这道习题的目的是帮助读者理解专用IP地址的特点。

（1）RFC1918提出了在A、B、C三类IP地址中，各保留一部分地址作为专用IP地址。专用地址用于不接入Internet的内部网络。内部网络的主机向Internet发送分组时，需要将专用地址转换成全局IP地址。

（2）表5-4给出了保留的专用地址。

表5-4 保留的专用地址

类	网络号	总数
A	10.	1
B	172.16～172.31	16
C	192.168.0～192.168.255	256

（3）如果一个组织出于安全等原因，希望组建一个专用的内部网络，不准备连接到Internet，或者在转发分组到Internet时希望使用网络地址转换（NAT）技术，那么该组织就可以使用专用IP地址。

因此，C的描述是正确的。

答案：C。

5-3-32 分析：设计这道习题的目的是为了加强读者对IP地址计算的能力。

（1）172.31.128.255/18是一个B类地址，前缀为18，除去B类地址的前16位，子网地址是2位，一个8位的二进制比特序列，前2位是10就是128，说明之后的6位只能是全0。所以第4个字节数是255，也不能是广播地址。因此，A属于单播地址。

（2）10.255.255.255是A类的广播地址，排除B。

（3）192.168.24.59/30是一个C类地址，前缀为30，59的二进制序列为001110 11，表明主机号2位为全1。因此，C也是广播地址。

（4）D类IP地址不标识网络，地址覆盖范围为224.0.0.0～239.255.255.255。D类IP地址用于其他特殊的用途，如多播地址。因此，D224.105.5.211不属于单播地址。

答案：A。

5-3-33 分析：设计这道习题的目的是为了加强读者对子网地址计算的能力。

路由器收到目的地址为212.26.17.4的分组，应该转发到哪个子网，就要看网络地址是否匹配。比较直接的办法是计算出不同子网地址的覆盖范围，就可以判断目的地址表示的主机在哪个子网中。

（1）子网地址为212.26.0.0/21，C类地址212.26.00000000.00000000，子网地址为21，主机地址为11，那么该子网地址范围：212.26.0.0～212.26.7.255。

（2）子网地址为212.26.16.0/20，C类地址212.26.00010000.00000000，子网地址为20，主机地址为12，那么该子网地址范围：212.26.16.0～212.26.31.255。

（3）子网地址为212.26.8.0/22，C类地址212.26.00001000.00000000，子网地址为

22,主机地址为 10,那么该子网地址范围：212.26.8.0～212.26.11.255。

(4) 子网地址为 212.26.20.0/22,C 类地址 212.26.00010100.00000000,子网地址为 20,主机地址为 12,那么该子网地址范围：212.26.20.0～212.26.23.255。

因此,目的地址为 212.26.17.4 的主机在 B 给出的子网中。

答案：B。

5-3-34 分析：设计该例题的目的是加深读者对网络地址转换 NAT 的理解。在讨论网络地址转换 NAT 时,需要注意以下几个主要问题：

(1) 网络地址转换 NAT 是 IP 地址重用与缓解 IP 地址短缺的有效方法。

(2) NAT 的基本思路是：为内部网络分配一个或少量的全局 IP 地址;内部网络的主机分配专用 IP 地址。如果内部网络的主机需要访问外部的 Internet 主机时,可以通过支持网络地址转换协议的 NAT 路由器,将内部专用 IP 地址转换成全局 IP 地址。

(3) 在电子政务、电子商务内部网络中常用的专用 IP 地址有 10.0.0.0/8 等。

(4) 实际应用的 NAT 软件中,通常将专用 IP 地址与传输层端口号结合起来转换。将 IP 地址与传输层端口号结合起来转换的过程如图 5-11 所示。

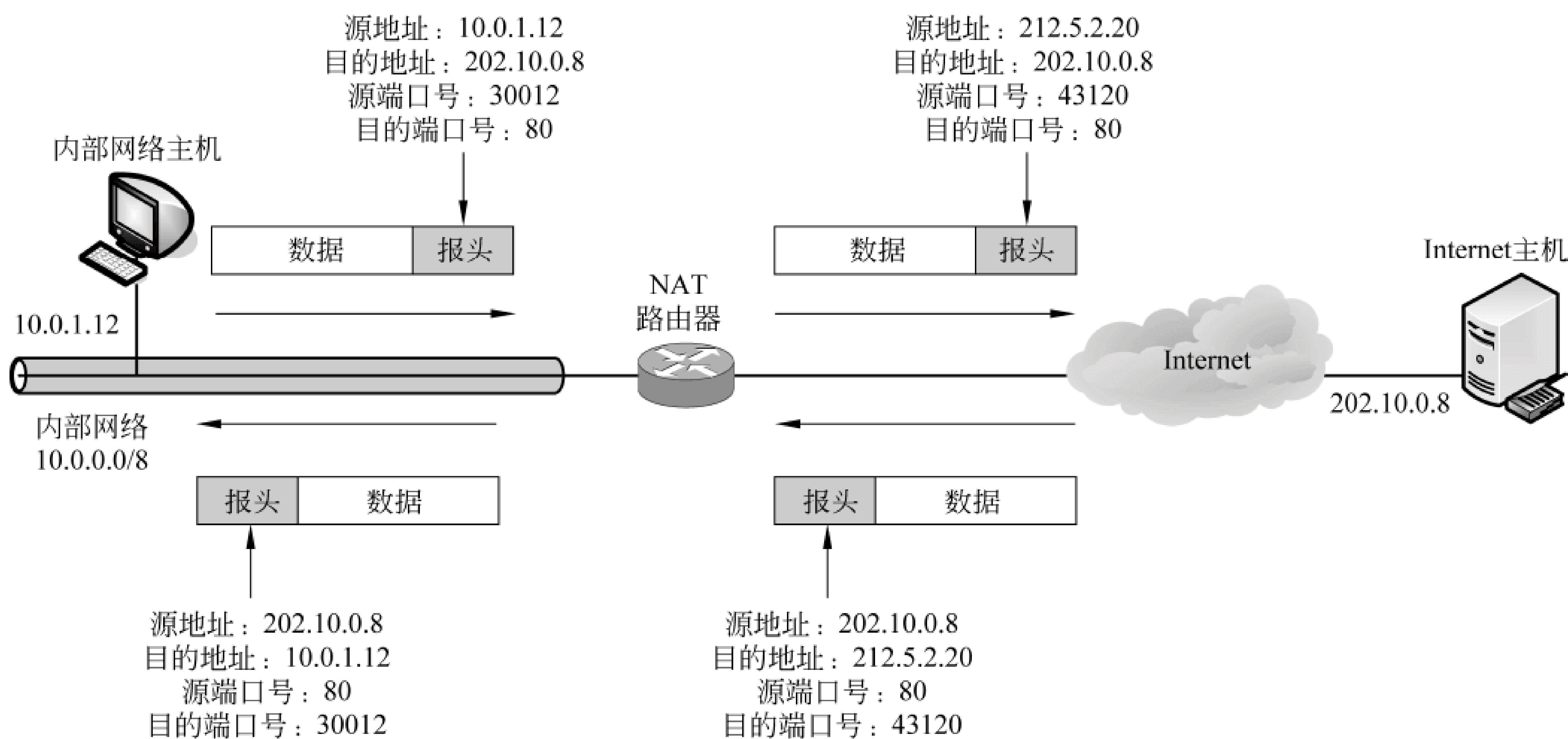


图 5-11 将 IP 地址与传输层端口号结合起来转换的过程示意图

在 NAT 路由器的内部网络一侧使用的是专用 IP 地址 10.0.0.0/8。以源地址为 10.0.1.12 发送的 IP 分组是不能被 Internet 中路由器所转发的。因此,以源地址为 10.0.1.12、目的地址为 202.10.0.8 的分组必须经过 NAT 路由器进行地址转换。图中转换后的分组源地址为 212.5.2.20,目的地址不变。同时,分组数据字段中的 TCP 源端口号也从 30012 转换成 43120,目的端口号不变。

从目的节点返回的分组源地址为 202.10.0.8、目的地址为 212.5.2.20。经过 NAT 路由器之后,源地址不变,目的地址还原成 10.0.1.12。同样,TCP 目的端口号也从 43120 还原为 30012,源端口号不变。

(5) NAT 可以分为"一对一"和"多对多"两类。实现地址"一对一"转换的方法属于静态 NAT,即配置一个内部专用 IP 地址对应一个公用的 IP 地址。如果属于前面例子中假设

的：每个内部网络的 100 个用户就可以共享 10 个全局 IP 地址，那么就属于动态 NAT。10 个共享的全局 IP 地址可以放在一个全局 IP 地址池中。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

5.4 路由选择算法与分组交付

5-4-1 分析：设计该例题的目的是加深读者对路由选择算法概念的理解。在讨论路由选择算法概念时，需要注意以下几个主要问题：

(1) "地址""路由"与"路由选择"是网络层重要的术语。"地址"标识着节点的位置；"路由"是分组从源节点到达目的节点的传输路径；"路由选择"是用来选择通过通信子网的合理传输路径；"路由选择算法"为路由器产生和不断更新、完善路由表提供了算法依据。路由选择是网络层的主要功能。

(2) 一个理想的路由选择算法应具有的特点是：算法必须是正确、稳定和公平的，算法应该尽量简单，算法必须能够适应网络拓扑和通信量的变化，算法应该是最佳的。

(3) 影响路由选择算法的参数主要是：

- 跳数(hop count)——一个分组从源节点到达目的节点经过的转发路由器的个数。
- 带宽(bandwidth)——链路的传输速率。
- 延时(delay)——一个分组从源节点到达目的节点花费的时间。
- 负载(load)——通过路由器或线路的单位时间通信量或吞吐量。
- 可靠性(reliability)——传输过程中的误码率。
- 开销(overhead)——一般是指传输过程中的花费。衡量开销的因素可以是链路长度、数据速率、链路容量、保密、传播延时与通信费用等。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

5-4-2 分析：设计该例题的目的是加深读者对分组交付的理解。分组交付与分组转发概念是相同的。在讨论分组交付时，需要注意以下几个主要问题：

(1) 分组交付是指在互联网络中路由器转发 IP 分组的机制。

(2) 分组交付要根据每个分组的源 IP 地址与目的 IP 地址来决定。

(3) 如果在同一子网的主机之间交换 IP 分组，它们可以不通过路由器，直接进行分组传输，那么它属于直接交付；如果两个主机不属于同一子网，那么它们之间的 IP 分组交换需要通过一个或多个路由器转发，这时它就属于间接交付。

(4) 是直接交付还是间接交付，路由器需要根据分组的目的 IP 地址与源 IP 地址是否属于同一网络来判断。

从以上分析中可以看出，网桥属于数据链路层的设备，在分组交付中不会涉及网桥。因此，A 的描述是错误的。

答案：A。

5-4-3 分析：设计该例题的目的是加深读者对路由器的组成和功能的理解。在讨论路由器的组成和功能时，需要注意以下几个主要问题：

(1) 路由器在网络层实现网络的互联。

(2) 路由器的主要服务功能是：建立并维护路由表，提供网络间的分组转发功能。

(3) 路由器结构可划分为两个部分：路由选择部分和分组转发部分。

(4) 路由选择部分核心构件是路由选择处理机。路由选择处理机的任务是根据所选定的路由选择协议构造路由表，同时从相邻路由器交换路由信息，更新和维护路由表。

(5) 分组转发部分由交换结构、一组输入端口和一组输出端口组成。

- 交换结构的作用就是根据转发表对分组进行处理，将某个输入端进入的分组从一个合适的输出端口转发出去。
- 路由器一般有多个输入端口和多个输出端口。在路由器的输入和输出端口中都各有3个模块，它们对应于物理层、数据链路层和网络层的处理模块。物理层进行比特流的接收与发送，数据链路层则按照数据链路层协议接收和发送帧，而网络层则处理分组信息。
- 当一个分组正在查找转发表时，后面又紧跟着从这个输入端口收到另一个分组，这个后到的分组就必须在输入队列中排队等待。输出端口从交换结构接收分组，然后将它们发送到路由器输出端口的线路上，也需要设有一个缓存并形成一个输出队列。

(6) 只要路由器的接收分组速率、处理分组速率、输出分组速率小于线速，无论是输入端口、处理分组过程与输出端口都会出现排队等待，产生分组转发延时，严重时会因为队列长度不够溢出，而造成分组丢失。

(7) 第三层交换机本质上是用硬件实现的一种高速路由器。

从以上分析中可以看出，A的描述是错误的。

答案：A。

5-4-4 分析：设计这道习题的目的是帮助读者理解一个IP分组经过路由器转发的过程中，源与目的IP地址不变，而源与目的MAC地址是变化的。

在路由器转发一个分组时，它的IP地址是不变的，但是MAC地址是变化的。在题目图中所示的情况下，分组1-2经过R1路由器转发时，源MAC地址是R1的Port2端口网卡的MAC地址02-A1-21-99-2B，而目的MAC地址应该是R2的Port1端口网卡的MAC地址B2-00-20-00-01。目的IP地址是不变的，为202.12.5.2。因此，B所示的目的IP地址202.12.5.2与目的MAC地址B2-00-20-00-01是正确的。

答案：B。

5-4-5 分析：设计该例题的目的是训练读者看懂网络结构图，同时通过生成一张简化路由表来加深读者对路由表形成的基本方法以及路由器工作原理的理解。

(1) 用于构造路由表的网络包括3个：LAN1、LAN2与LAN3，其中2个为B类网络，1个为C类网络。

(2) 路由器R1与R3用一个串行链路连接。

(3) 图中没有标出子网掩码，应作为没有划分子网的情况对待，使用标准分类地址的掩码。

(4) 路由器R2接入Internet，那么134.18.5.2自然是R1的默认路由。

(5) 从路由器R1看，它必须在路由表中表示到3个局域网的路由，以及一个默认路由，因此R1的路由表应该包括4项内容。

解答：R1 路由表如表 5-5 所示。

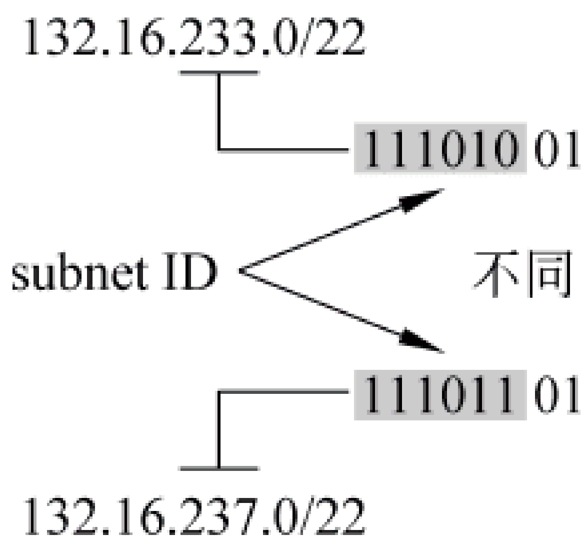
表 5-5　R1 路由表

掩　　码	目 的 地 址	下一跳地址	转发端口
255.255.0.0	134.18.0.0	—	m0
255.255.0.0	129.8.0.0	222.13.15.40	m1
255.255.255.0	220.3.5.0	222.13.15.40	m1
0.0.0.0	0.0.0.0	134.18.5.2	m0

5-4-6　分析：设计这个例题的目的是加深读者对于路由器按照“最长前缀匹配规则”转发分组的工作原理的理解。当路由器接收到一个分组时，它首先是判断是该分组的目的地址是不是特殊地址；如果不是，那么是直接交付还是间接交付；如果是间接交付，则需要根据目的地址在路由器转发表寻找“最长前缀匹配”项，以确定转发的端口。

计算：

(1) 分组的目的 IP 地址为 132.19.237.5，按照惯常的思维首先会选择 132.19.233.0/22 进行比较。



比较的结果发现：由于两者的子网地址不同，因此判断 132.19.237.5 不在 132.19.233.0/22 的子网内，不能够通过这个端口转发。

(2) 分组的目的 IP 地址为 132.19.237.5，那么 132.0.0.0/8 与 132.19.0.0/11 都可以转发。如果将 132.19.237.5 与 132.0.0.0/8 比较，相同的前缀长度为 8，而 132.19.237.5 与 132.19.0.0/11 相同的前缀达到 11。因此，根据“最长前缀匹配规则”转发分组的原则，应该选择 E1 为转发端口。

答案：最佳路由是通过 E1 端口转发。

5-4-7　分析：

(1) 这是一道关于 IP 地址与路由的综合练习题。设计这道例题主要是考核读者对 IP 地址的概念、子网划分与子网地址分配方法、路由汇聚、路由表构造等知识掌握的情况和灵活应用的能力。

在读懂前面各道例题之后，完成该例题的知识与技能都已经掌握。由于这是一道设计题，解决这个问题有较大的灵活性，答案也不是唯一的。

(2) 考试时读者首先要根据题意与图中的标识，按照网络中一些规定，获取一些有价值的信息，在此基础上形成解决该问题的思路。

从题目图可以获得以下的信息：

① 校园网获得的是一个 202.15.20.0/24 的标准 C 类 IP 地址，需要对 C 类地址进行子

网划分。标准C类IP地址的掩码为24。

② 在进行子网划分时,首先要分析校园网中需要哪些地址。

第1部分是LAN1、LAN2与LAN3,题中说明每个局域网中最多要连接60台计算机或服务器,加上局域网与路由器连接的接口,每个局域网至少需要61个IP地址。

第2部分是路由器R1的接口0与R2的接口0需要分配IP地址。

第3部分是路由器R1的接口1与R3的接口1需要分配IP地址。

③ 标准C类IP地址的掩码为24,可用于子网划分的地址只能借用202.15.20.0中第4字节的若干位。

这里需要注意的是:在早期的RFC950文档规定中,子网号为全0和全1的不能分配给子网,但是在无类别域间路由CIDR中用前缀表示地址块的范围,子网号为全0和全1的地址可以分配给子网,但是主机号全0的网络地址、全1的广播地址不能分配给主机。实际的校园网地址规划中常常会涉及这个问题。

(3) 规划方法。

① 已知:要求每个局域网至少需要61个IP地址,那么必须保留第4字节的后6位作为主机地址hostID,可以借用2位作为子网地址subnetID。

如图5-12所示,24位的netID与2位的subnetID构成了子网的26位的前缀。那么,LAN1地址为202.15.20.0/26,LAN2地址为202.15.20.64/26,除去主机号hostID全0和全1之外的IP地址都可以分配给主机与路由器。同时,可以将202.15.20.128/26分配给LAN3作为服务器的IP地址。

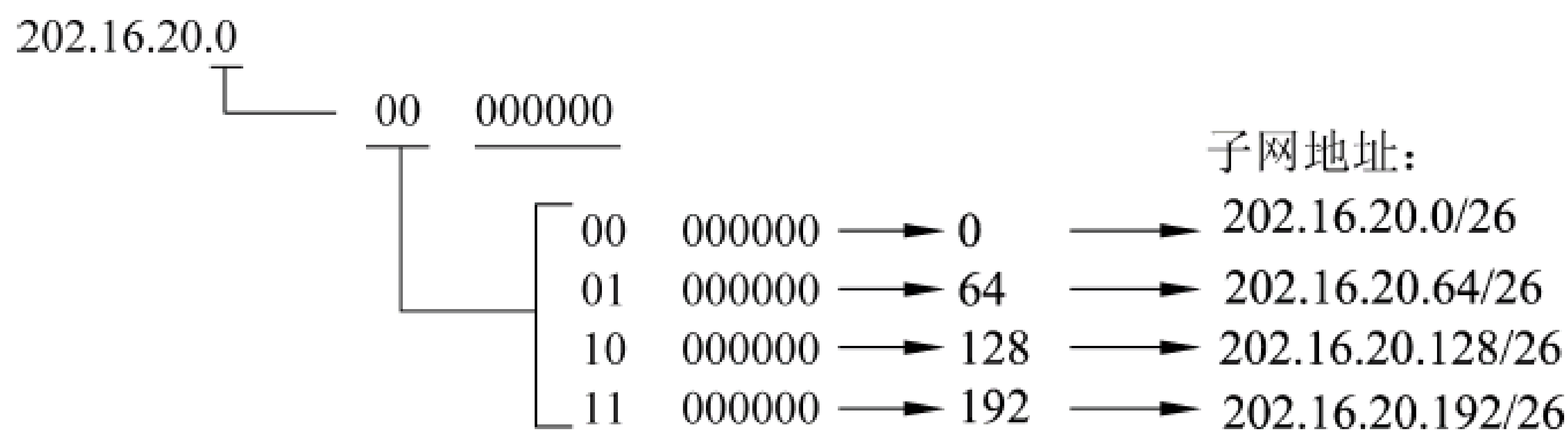


图5-12 子网划分示意图

② 剩下的地址段是202.15.20.192/26分配给两段直接连接R1-R2、R1-R3的串行链路接口,需要采取CIDR的方法,按不同的掩码分隔出两个不同的地址块来处理。

计算:

(1) 子网划分。

要求每个局域网中最多要连接60台计算机,加上局域网与路由器连接的接口,每个局域网至少需要61个IP地址,因此必须首先保证主机地址数量足够,那么需要保留IP地址中第4个字节的后6位为主机号;第4个字节的前2位作为子网号。网络前缀应该为26。

① LAN1的地址为202.15.20.0/26,除去主机号全0(202.15.20.0)与主机号全1(202.15.20.63)之外的所有地址可以在LAN1中分配。

地址范围为202.15.20.1~202.15.20.62。

将202.15.20.1/26地址分配给路由器R2接口1。

② LAN2的地址为202.15.20.64/26,除去主机号全0(202.15.20.64)与主机号全1(202.15.20.127)之外的所有地址可以在LAN2中分配。

地址范围为 202.15.20.65～202.15.20.126。

③ LAN3 的地址为 202.15.20.128/26，除去主机号全 0(202.15.20.128)与主机号全 1(202.15.20.191)之外的所有地址可以在 LAN3 中分配。

地址范围为 202.15.20.129～202.15.20.190。

④ 将 202.15.20.192/26 地址分配给直接连接 R1-R2、R1-R3 接口的两段串行链路，需要采取 CIDR 的方法，使用不同的掩码来分隔不同的地址块。最直观的方法是将 202.15.20.192/26 按照 30 位前缀，划分为两个地址块。

(2) IP 地址规划。

图 5-13 是第 1 个地址块(202.15.20.252/30)划分示意图，将其中的 202.15.20.253/30 地址分配给路由器 R1 的接口 0；将 202.15.20.254/30 地址分配给路由器 R2 的接口 0。

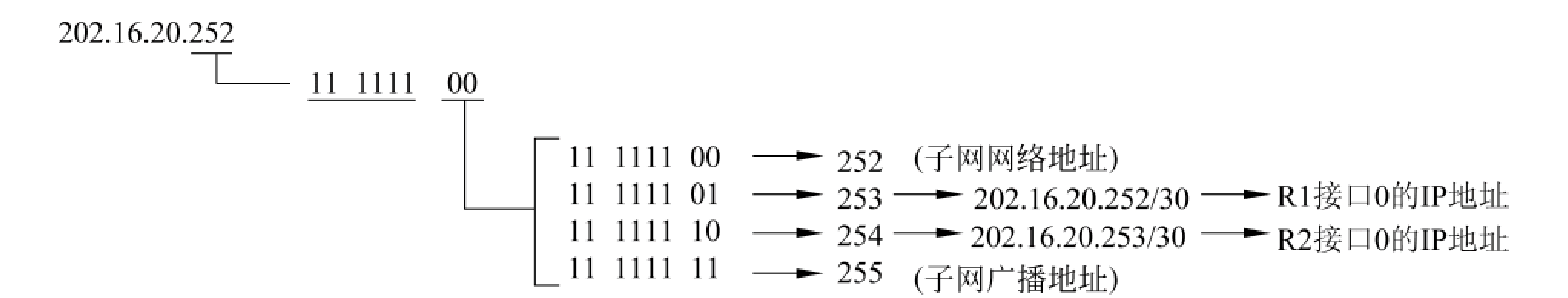


图 5-13 第 1 个地址块(202.15.20.252/30)的划分

图 5-14 是第 2 个地址块(202.15.20.192/30)的划分示意图，将其中的 202.15.20.193/30 地址分配给路由器 R1 的接口 1；将 202.15.20.194/30 地址分配给路由器 R3 的接口 1。

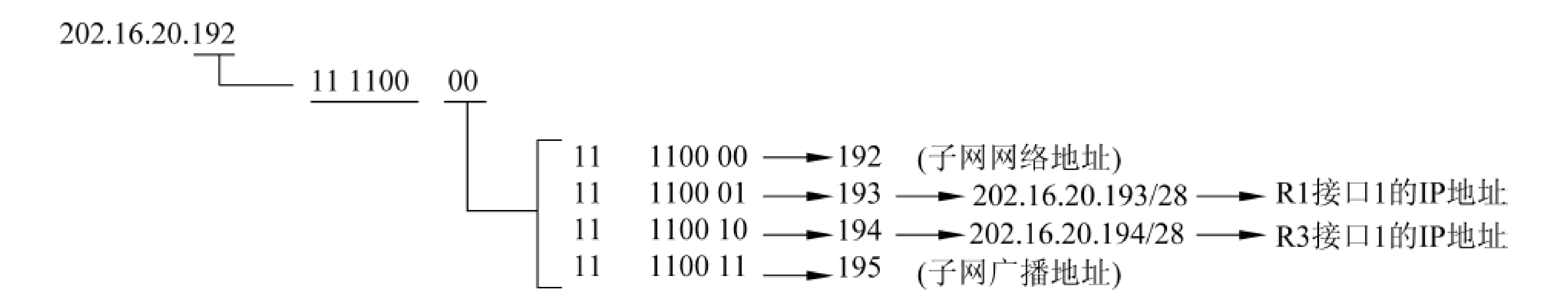


图 5-14 第 2 个地址块(202.15.20.192/30)的划分

按照以上思路规划的 IP 地址结构如图 5-15 所示。

答案：

(1) 子网划分后的 LAN1、LAN2、LAN3 的主机 IP 地址范围：

LAN1 地址范围为 202.15.20.1～202.15.20.62。

LAN2 地址范围为 202.15.20.65～202.15.20.126。

LAN3 地址范围为 202.15.20.129～202.15.20.190。

(2) 路由器 R2 的路由表如表 5-6 所示。

表 5-6 路由器 R2 的路由表

目的 IP 地址	子网掩码	下一跳 IP 地址	转发接口
202.15.20.0	255.255.255.192	直接连接	1
202.15.20.64	255.255.255.192	直接连接	2
0.0.0.0	0.0.0.0	202.15.20.254	0

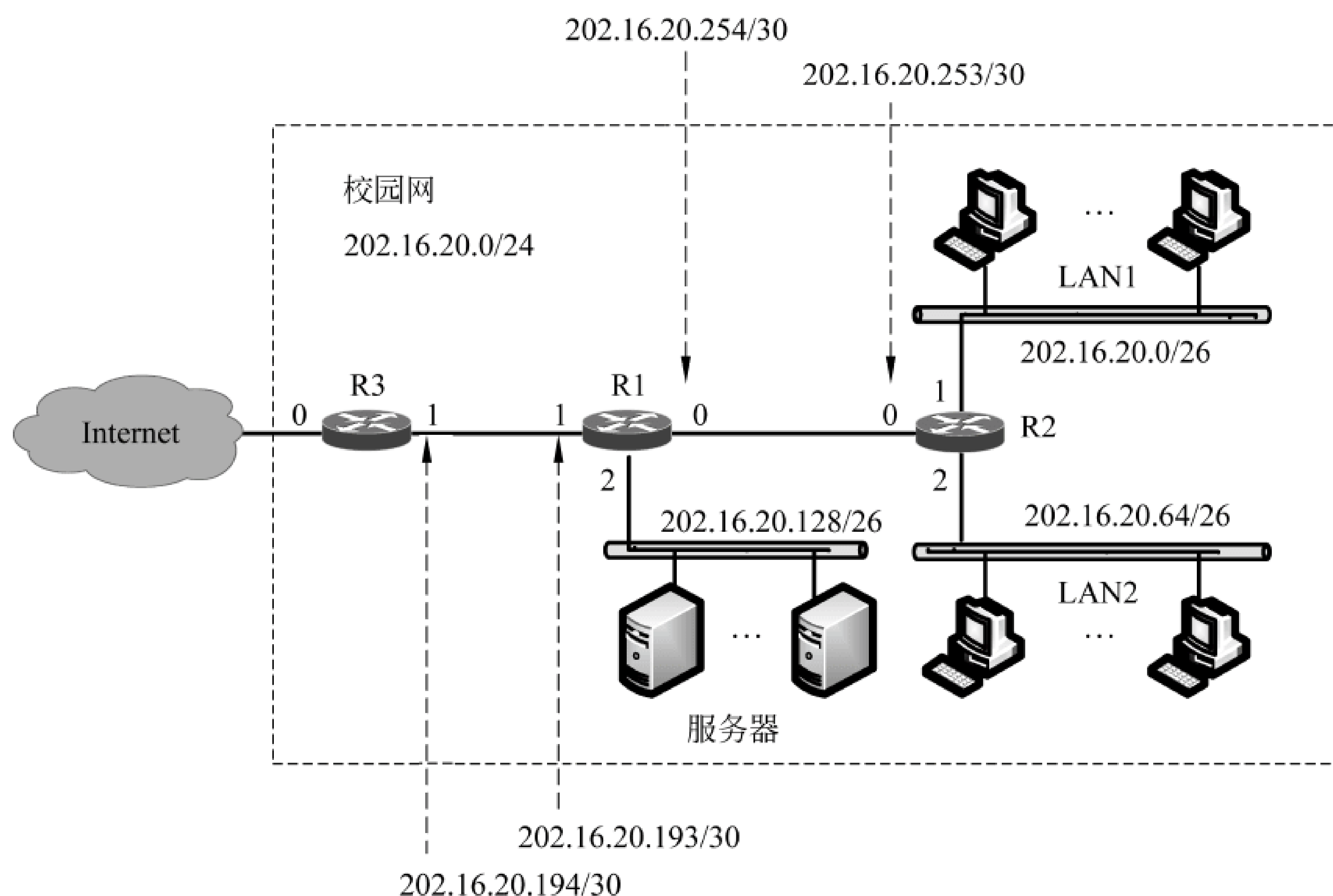


图 5-15 IP 地址分配情况

(3) 地址汇聚后的路由器 R1 的路由表。

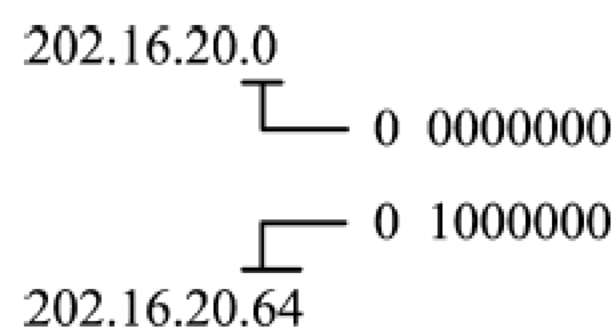


图 5-16 地址汇聚

由于 LAN1 的地址为 202.15.20.0/26,LAN2 的地址为 202.15.20.64/26,需要对它们进行地址汇聚。地址汇聚过程如图 5-16 所示。

从图 5-16 可以看出,汇聚后的网络前缀长度应该为 25,对应的掩码为 255.255.255.128。

路由器 R1 的路由表如表 5-7 所示。

表 5-7 路由器 R1 的路由表

目的 IP 地址	子网掩码	下一跳 IP 地址	转发接口
202.15.20.0	255.255.255.128	202.15.20.253	0
202.15.20.128	255.255.255.192	直接连接	2
0.0.0.0	0.0.0.0	202.15.20.194	1

5-4-8 分析:设计这道例题的目的,一是帮助读者了解和熟悉各种网络考试的题型,二是帮助读者熟悉关于路由表的常用的几种表述习惯。本题的解答需要掌握以下的知识点:

(1) 第一个问题是根据"最长前缀匹配原则",在路由表中为一个分组寻找适当的转发端口。对"最长前缀匹配原则"的理解应该是:将一个目的地址与子网地址比较,可能有多个子网的地址可以匹配,那么需要选择匹配的前缀最长的那个子网。

解决这个问题的时候,可将符合题目给出路由表的网络结构想象为图 5-17 的形式。

由于是 B 类 IP 地址,比较 4 个路由表项与分组的目的地址,那么最简捷的方法是依据前缀长度/30、/28 与/16,判断分组的目的地址在哪个子网地址中。这样就可以比较准确地找出转发分组的输出端口。

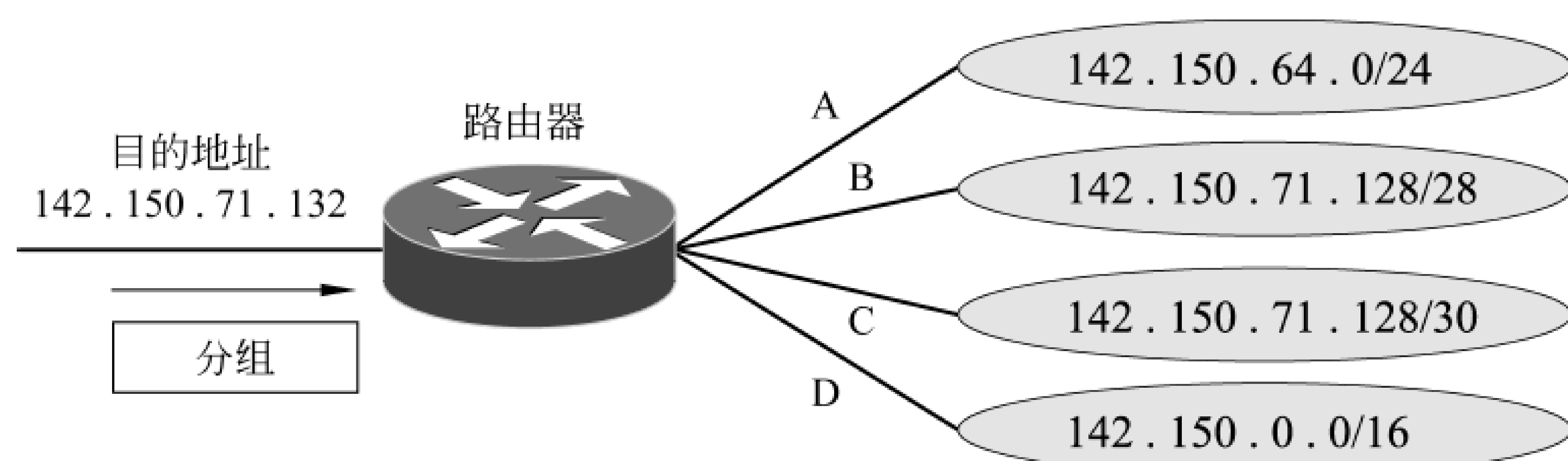


图 5-17　符合题目给出路由表的网络结构

(2) 如果在路由表中增加一条表项，使得 142.150.71.132 为目的地址的分组选择 A 作为下一跳的输出端口，并且不影响其他目的地址 IP 分组的转发。

满足题意要求的方案有两种可能。一是在 142.150.71.128/28、142.150.71.128/30 的基础上，选择子网的前缀为 29(大于 28)的子网地址，或者是子网的前缀为 31(大于 30)的子网地址，这要具体分析地址结构后确定。一般情况下，第一种可能性最大。二是根据 142.150.71.132 重新设计一个能够满足题意要求的子网地址。

(3) 在路由表中增加一个表项，使得所有目的地址与路由表中表项不匹配的 IP 分组的下一跳都是 E。由于原路由表中输出端口没用 E，因此问题变得很简单，这就是经常在路由表中看到的对应地址：0.0.0.0，下一跳：E。

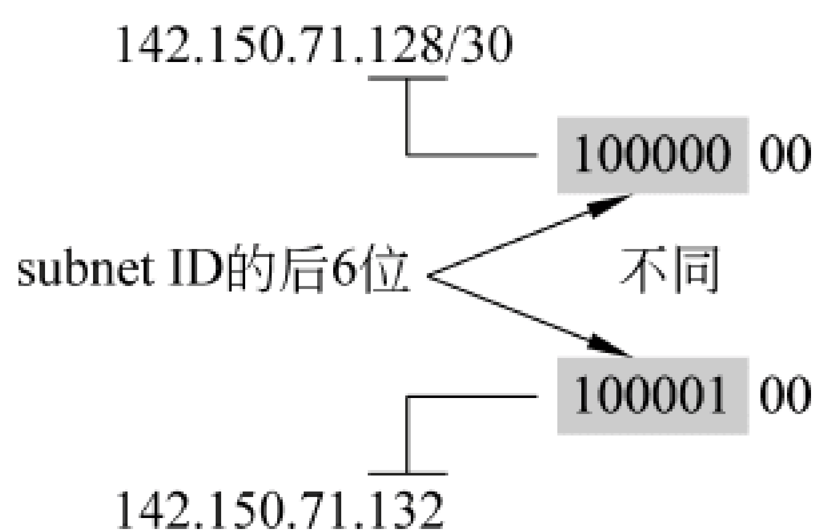
(4) 将 142.150.64.0/24 划分为 4 个规模尽可能长的等长子网，那么只可能是借主机号 8 位中的 2 位作为子网号，子网掩码为 26，形成新的子网地址为 142.150.64.0/26。在此基础上给出每个子网可以分配的地址范围。

计算：

(1) 判断目的地址为 142.150.71.132 的分组转发端口。

① 分析：142.150. 71.128/30。

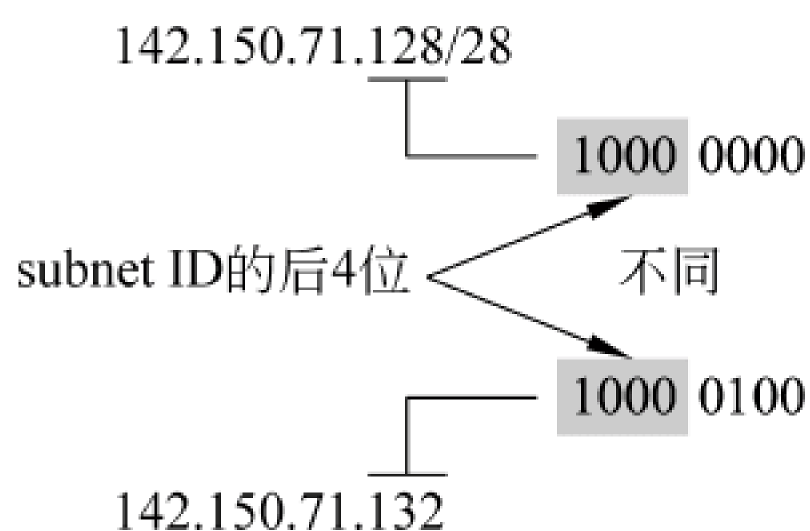
142.150. 71.128/30 的前缀是 30。比较 142.150.71.128/30 与 142.150.71.132，它们的前 2 个字节相同，只需要比较第 4 个字节的前 6 位。



比较的结果是不相同，不属于 142.150.64.0/30 标识的子网地址，需要往下比较。

② 分析：142.150.71.128/28。

142.150.71.128/28 的前缀是 28。比较 142.150.71.128/128 与 142.150.71.132，它们的前 3 个字节相同，只需要比较第 4 个字节的前 4 位。



比较的结果相同,目的地址属于142.150.71.128/28标识的子网地址,分组转发的下一跳端口应该为B。

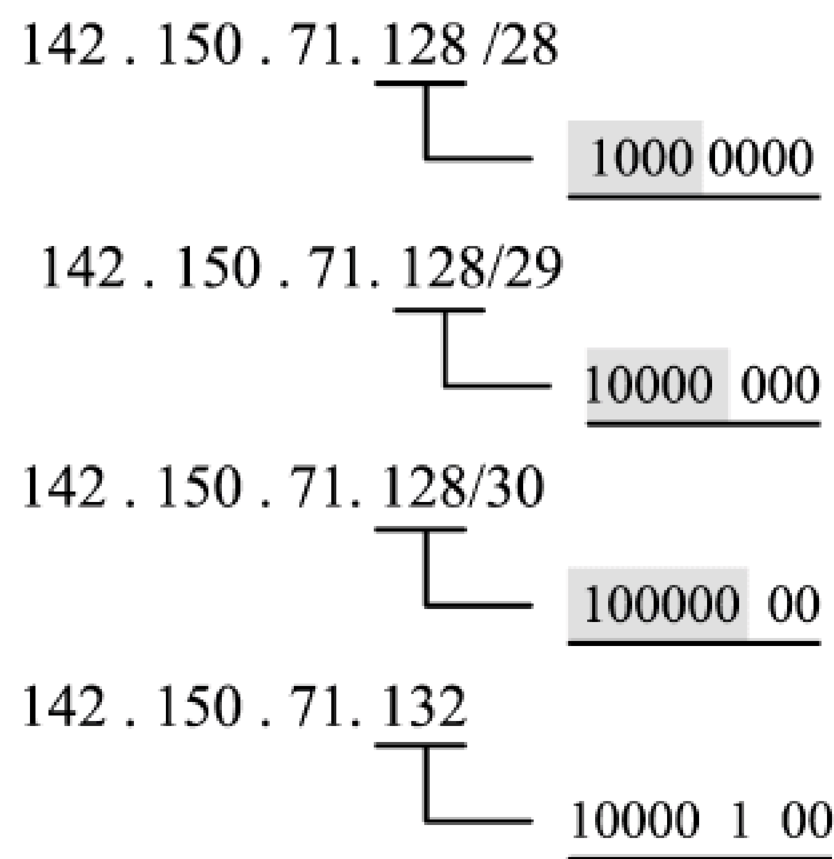


图5-18 地址比较

(2) 题目要求目的地址为142.150.71.132的分组通过端口A,而又不影响其他目的地址的分组转发,如果存在142.150.71.128/28、142.150.71.128/29、142.150.71.128/30共3个子网,那么需要根据"最长前缀匹配原则",将142.150.71.132与142.150.71.128/28、142.150.71.128/29、142.150.71.128/30进行比较,找出了"最长前缀匹配"的子网,确定转发端口。比较的过程如图5-18所示。

分析:

① 当目的地址为142.150.71.132的分组到达时,按照"最长前缀匹配原则",它应该选择142.150.71.128/29。因为这个匹配的子网地址前缀长度为29,比142.150.71.128/28要长。只要在路由表中增加一项:142.150.64.0/29,下一跳端口为A,就可以满足题目的要求。那么这样的网络结构如图5-19所示。

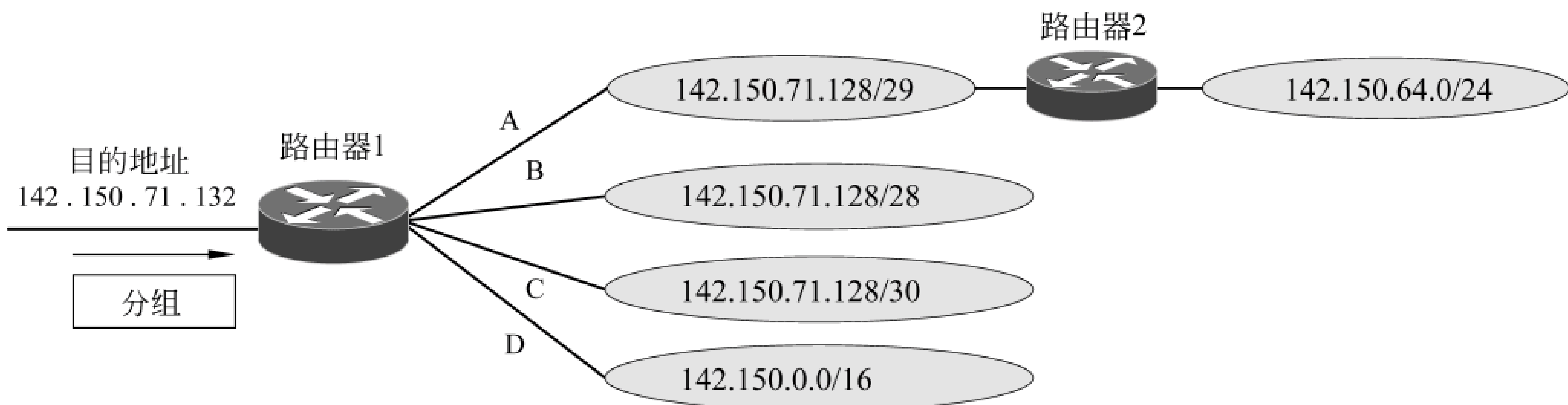


图5-19 符合题意的网络结构

② 如果要在路由表中增加一项:142.150.71.132/30,下一跳端口为A,也可以满足题目的要求。那么这样的网络结构如图5-20所示。从地址结构的比较中可以看出,当目的地址为142.150.71.132的分组到达时,按照"最长前缀匹配原则",它应该选择142.150.71.132/30,而不会选择其他的输出端口。

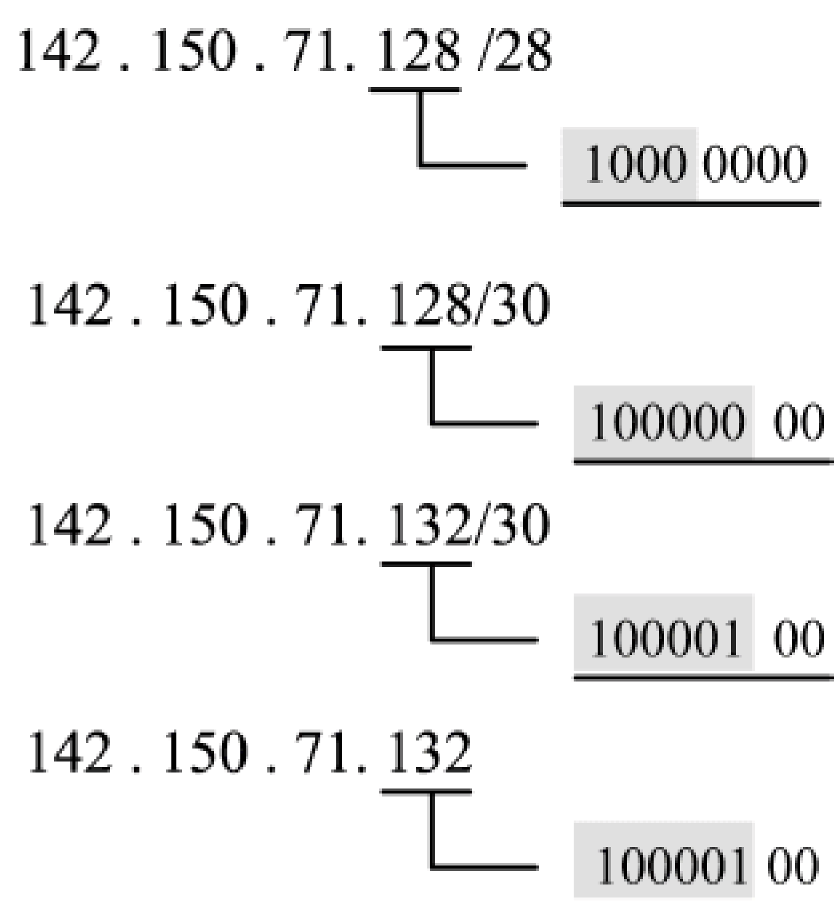
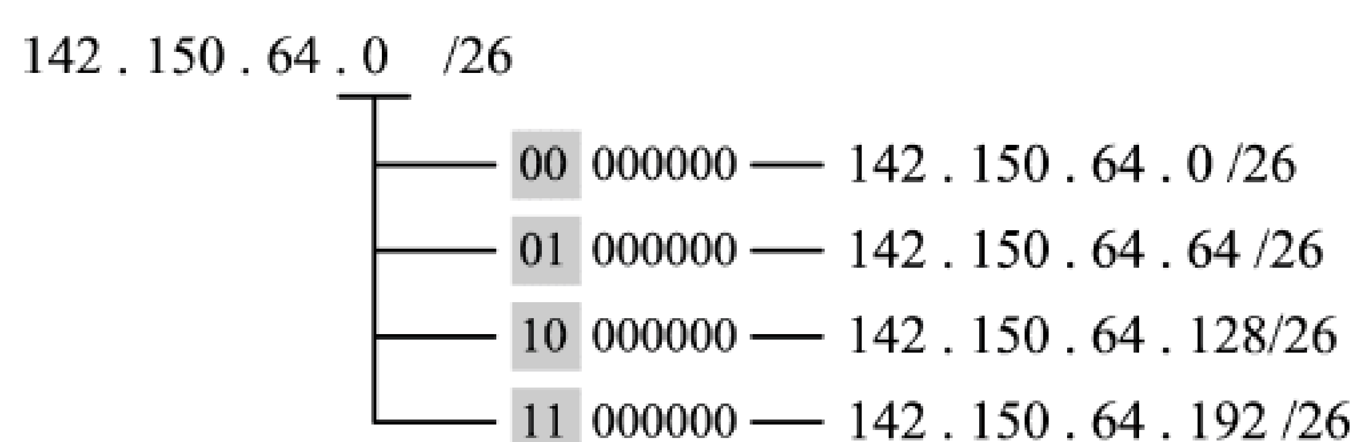


图5-20 增加一项142.150.71.132/30的地址结构比较

(3) 在路由表中增加一个表项,使得所有目的地址与路由表中表项不匹配的IP分组的下一跳都是E。由于原路由表中输出端口没用E,因此问题变得很简单,这就是经常在路由表中增加一个表项:网络地址 0.0.0.0,下一跳:E。

(4) 将142.150.64.0/24划分为4个规模尽可能大的等长子网,那么只可能是借主机号8位中的2位作为子网号,子网掩码为26,形成新的子网地址为142.150.64.0/26。



每个子网可以分配的地址范围为：

子网1　142.150.64.1～142.150.64.63

子网2　142.150.64.65～142.150.64.127

子网3　142.150.64.129～142.150.64.191

子网4　142.150.64.193～142.150.64.255

答案：

(1) 分组转发的下一跳端口为B。

(2) 增加一个表项：142.150.71.128/29，下一跳：A。

或增加一个表项：142.150.71.132/30，下一跳：A。

(3) 增加一个表项：0.0.0.0，下一跳：E。

(4) 子网可以分配的地址范围为：

子网1　142.150.64.1～142.150.64.62

子网2　142.150.64.65～142.150.64.126

子网3　142.150.64.129～142.150.64.190

子网4　142.150.64.193～142.150.64.254

5-4-9　分析：设计这道习题的目的是加深读者对路由器与路由表的理解。

已知：互联了3个子网的网络拓扑如图5-21所示。

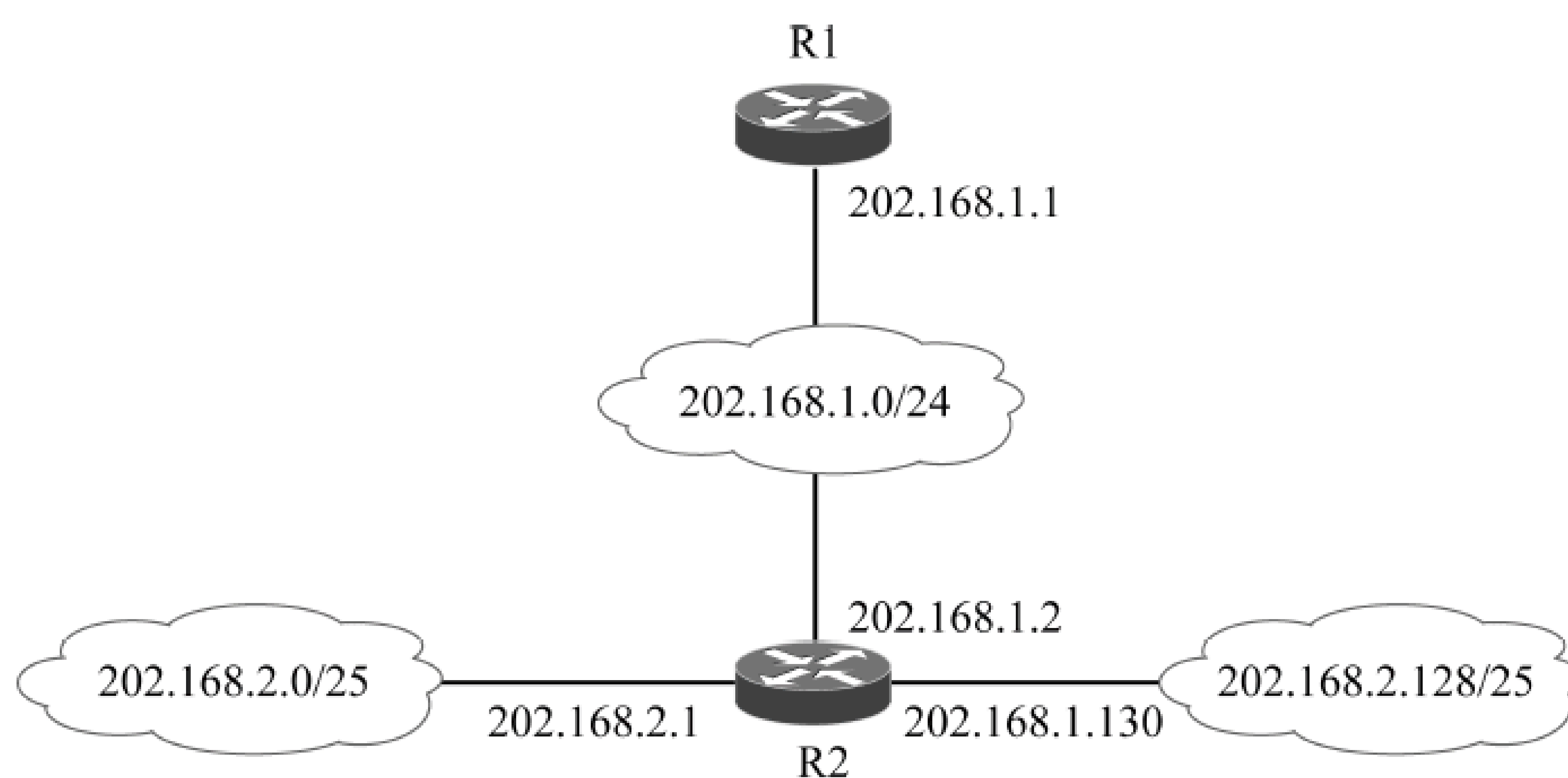


图5-21　互联3个子网的网络拓扑

(1) 这个网络中有3个子网：202.168.1.0/24、202.168.2.0/25、202.168.2.128/25。路由器R1只有到达子网202.168.1.0/24的路由，还需要增加到另外两个子网的路由。

(2) 能够到达202.168.2.0/25，202.168.2.128/25子网的路由应该由这两个地址汇聚而成。计算202.168.2.0/25，202.168.2.128/25汇聚后的地址为：202.168.2.0/24。

(3) 按照路由表项(目的网络、子网掩码、下一跳)的要求：

目的网络为202.168.2.0；

子网掩码为 255.255.255.0;

下一跳为 202.168.1.2。

答案:为 R1 增加一条路由为"202.168.2.0 255.255.255.0 202.168.1.2"。

5-4-10 分析:设计这道习题的目的是加深读者对路由器与路由表的理解。

题目给出路由器不完整的路由表如表 5-8 所示。

表 5-8 题目给出的路由表

序号	目的网络	子网掩码	下一跳	转发端口
1	176.11.64.0	255.255.240.0	R1 端口 1	端口 2
2	176.11.16.0	255.255.240.0	直接交付	端口 1
3	176.11.32.0	255.255.240.0	直接交付	端口 2
4	176.11.48.0	255.255.240.0	直接交付	端口 3
5	0.0.0.0	0.0.0.0	R2 端口 2	端口 1

(1) 表中序号 1~4 的目的地址 176.11.64.0、176.11.16.0、176.11.32.0 与 176.11.48.0 都属于 B 类地址,掩码为 255.255.0.0,因此它们由 176.11.0.0 划分出来的。

(2) 根据路由器 R 的路由表判断网络结构。

① 从路由表中序号 2、3 的记录中可以看出,176.11.16.0、176.11.32.0 与 176.11.48.0 是从路由器 R 的端口 2、端口 2 与端口 3 直接交付,那么路由器 R 的端口 1 连接地址为 176.11.16.0 的子网;端口 2 连接着地址为 176.11.32.0/20 的子网,端口 3 连接着地址为 176.11.48.0/20 的子网。

② 从 R 转发到地址为 176.11.64.0 子网的分组,下一跳是 R1 端口 1,那么路由器 R1 连接在 176.11.32.0 子网上,端口 1 的地址应该是 176.11.32.5。

③ 目的地址为 0.0.0.0、子网掩码为 0.0.0.0,是一条默认路由,下一跳是 R2 的端口 1,那么路由器 R2 连接在 176.11.16.0 子网上,端口 1 的地址应该是 176.11.32.5。凡是目的地址不在路由表中,那么分组的默认路由的下一跳是 R2 的端口 2。R2 的端口 2 的地址为 176.11.16.5。

根据这样的路由表结构,大致可以判断网络结构如图 5-22 所示。

(3) 目的主机 H1~H6 的下一跳地址。

① H1:21.13.24.78,路由表中没有目的地址,选择默认路由,下一跳为 R2 的端口 2,下一跳 IP 地址为 176.11.16.5。

② H2:176.11.64.129 属于子网 176.11.64.0,下一跳为 R1 的端口 1,下一跳 IP 地址为 176.11.32.5。

③ H3:176.11.35.72 属于子网 176.11.32.0,由 R 端口 2 直接交付。

④ H4:176.11.31.168 属于子网 176.11.32.0,由 R 端口 1 直接交付。

⑤ H5:176.11.60.239 属于子网 176.11.48.0,由 R 端口 3 直接交付。

⑥ H6:192.36.8.73 路由表中没有目的地址,选择默认路由,下一跳为 R2 的端口 2,下一跳 IP 地址为 176.11.16.5。

答案:

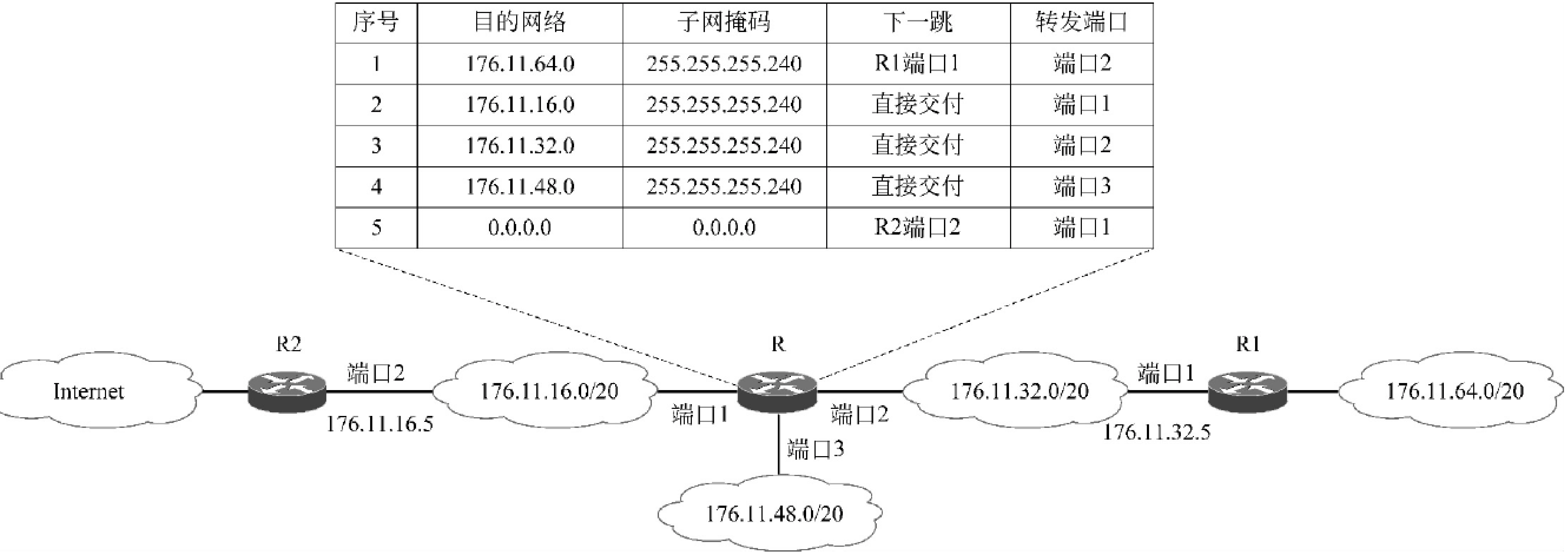


图 5-22 网络结构示意图

(1) 表中序号 1～4 的目的地址 176.11.64.0、176.11.16.0、176.11.32.0 与 176.11.48.0 都属于 B 类地址,掩码为 255.255.0.0,因此它们是由 176.11.0.0 划分出来的。

(2) R1 端口 1 的地址是 176.11.32.5。R2 的端口 2 的地址为 176.11.16.5。

(3) H1:21.13.24.78 下一跳为 R2 的端口 2,下一跳 IP 地址为 176.11.16.5。

H2:176.11.64.129 下一跳为 R1 的端口 1,下一跳 IP 地址为 176.11.32.5。

H3:176.11.35.72 由 R 端口 2 直接交付。

H4:176.11.31.168 由 R 端口 1 直接交付。

H5:176.11.60.239 由 R 端口 3 直接交付。

H6:192.36.8.73 下一跳为 R2 的端口 2,下一跳 IP 地址为 176.11.16.5。

5-4-11 分析:设计该例题的目的是加深读者对路由选择算法分类的理解。在讨论路由选择算法分类时,需要注意以下几个主要问题:

(1) 从路由选择算法对网络拓扑和通信量变化的自适应能力的角度划分,可以分为静态路由选择算法与动态路由选择算法两大类。

(2) 静态路由选择算法称为非自适应路由选择算法,其特点是简单和开销较小,但不能及时适应网络状态的变化。

(3) 动态路由选择算法称为自适应路由选择算法,其特点是能较好地适应网络状态的变化,但实现起来较为复杂,开销也比较大。

(4) 所有连接在互联网络中的路由器都要建立和维护一个路由表。路由表可以是静态的,也可以是动态的。

(5) 静态路由表。

静态路由表是由人工方式建立的,网络管理人员将每个目的地址的路径输入到路由表中。网络结构发生变化时,路由表无法自动更新。静态路由表的更新工作必须由管理员手工修改。因此,静态路由表一般只用在小型的、结构不会经常改变的局域网中,或者是故障查找的试验网络中。

(6) 动态路由表。

大型互联网络通常采用动态路由表。在网络系统运行时,系统将自动运行动态路由选择协议,建立路由表。当 Internet 结构变化时,例如某个路由器出现故障或某条链路中断,动态路由选择协议就会自动更新所有路由器中的路由表。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

5-4-12 分析:设计该例题的目的是加深读者对距离-向量路由算法特点的理解。在讨论距离-向量路由算法特点时,需要注意以下几个主要问题:

(1) 距离-向量路由算法(Bellman-Ford 算法)是一种典型的动态路由算法,是内部网络中应用广泛的路由选择算法之一。

(2) 距离-向量路由算法基本方法是:

① 每个路由器维护一张路由表。路由表中列出当前已知的到每个目的网络的输出端口与距离。

② 距离是到达目的节点跳数(或时间)的估算值。

③ 通过与相邻路由器相互交换路由信息来不断更新路由表。

(3) 距离-向量路由算法的缺点：

① 距离-向量路由算法限制在15跳以内，不适用于大型网络。

② 距离-向量路由算法需要较长的时间才能够收敛到稳定状态。

从以上分析中可以看出，A的描述是错误的。

答案：A。

5-4-13 分析：设计该例题的目的是加深读者对距离-向量路由算法对路由表更新过程的理解。在讨论距离-向量路由算法更新路由表时，需要注意以下几个主要问题：

(1) 路由表的建立。

当路由器刚启动时，对其(V,D)路由表进行初始化。初始化的路由器只包含所有与该路由器直接相连的网络的路由。由于是直接相连的网络，不需要经过中间路由器的转接，所以初始(V,D)寻径表中各路由的距离均为0。

(2) 路由表信息的更新。

在路由表建立之后，各路由器周期性地向外广播其(V,D)路由表的内容。如图5-23所示，路由器1与路由器2是一个自治系统中相邻的两个路由器。路由器1接收到路由器2发送的(V,D)报文，路由器1按照以下规律更新路由表的信息：

① 如果路由器1的路由表没有这项记录，路由器1在路由表中增加该项，由于要经过下一跳路由器2转发，因此距离D值加1。

② 如果路由器1的路由表的一项记录比路由器2发送的一项记录的距离D值减1还要大，路由器1在路由表中修改该项，距离D值根据路由器2提供的值加1。

答案：基于距离-向量算法更新后的路由表如图5-23所示。

目的网络	距离	路由
10.0.0.0	0	直接
20.0.0.0	5	路由器2
30.0.0.0	3	路由器2
40.0.0.0	8	路由器2
120.0.0.0	6	路由器2
125.0.0.0	4	路由器5
212.0.0.0	10	路由器6
220.0.0.0	9	路由器6

图5-23 更新后的路由器1路由表

5-4-14 分析：设计该例题的目的是加深读者对链路状态路由算法的理解。在讨论链路状态路由算法时，需要注意以下几个主要问题：

(1) 由于距离-向量路由算法收敛较慢，因此人们希望用链路状态路由算法去取得距离-向量路由算法。

(2) 链路状态路由算法要求每个路由器完成以下工作：

① 发现相邻路由器，并知道它们的IP地址。

② 测量到各个相邻路由器的延时或开销。

③ 构造一个分组，分组中包含所有刚得到的路由信息。

④ 将这个分组发送到自治系统内部所有的路由器。

⑤ 计算出到每个其他路由器的最短路径。

(3) 链路状态路由算法与距离-向量路由算法的区别：当路由状态发生变化时，链路状态路由算法要将刚得到的路由信息，通过一个IP分组通知到自治系统内部所有的路由器。因此，D的描述是错误的。

答案：D。

5-4-15 分析：设计该例题的目的是加深读者对分层路由概念的理解。在讨论分层路由概念时，需要注意以下几个主要问题：

(1) 随着网络规模的扩大，路由器的路由表存储的路由信息也随之快速膨胀，这将造成路由器工作效率急剧降低。为了适应网络规模扩大的需要，有必要采取分层路由的方法。

(2) 根据分层路由的需要，人们将路由器划分成区域，路由器只需要知道将分组发送到本区域目的节点的路径，对区域之外的路径可以不知道。

(3) 对于大型网络系统，可以采取多层路由的划分方法，继续将区域(region)划分为群(cluster)，将群划分为区(zone)，将区划分为组(group)。

(4) 到底应该划分为多少层为好，研究结果表明：对于一个包含 N 个路由器的网络，最优的级数为 $\ln N$。由于分层导致的平均路径长度的增长通常很小，因此分层是可以接受的。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

5-4-16 分析：设计该例题的目的是加深读者对自治系统基本概念的理解。在讨论自治系统的基本概念时，需要注意以下几个主要问题：

(1) Internet 采用分层的路由选择协议，它将整个 Internet 划分为许多较小的自治系统(AS)。一个自治系统内的所有网络都属于一个行政单位，例如一所大学、一个公司、政府的一个部门。自治系统的核心是路由的“自治”。

(2) 一个自治系统最重要的特点是它有权自主决定在本系统内应采用何种路由选择协议。自治系统内部的路由选择称为域内路由选择，自治系统之间的路由选择称为域间路由选择。

(3) 自治系统的概念的提出，实际上是将 Internet 分成两层。

① 一层是自治系统的内部网络，可以把它称为第一层区域，自治系统的内部路由器完成第一层区域的主机之间的分组交换。一个自治系统管理内部的路由器，通过一个主干路由器接入到主干区域(backbone area)。

② 连接自治系统的主干路由器构成主干区域，即 Internet 的第二层。第一层区域之间的分组交换是通过主干路由器实现的。

(4) 自治系统内部的路由器了解内部全部网络的路由信息，并能够通过一条路径将发送到其他自治系统的分组传送到连接本自治系统的主干路由器。自治系统内部的路由器要向主干路由器报告内部路由信息。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

5-4-17 分析：设计该例题的目的是加深读者对域内路由与域间路由概念的理解。在讨论域内路由与域间路由时，需要注意以下几个主要问题：

(1) 自治系统内部的路由选择称为域内路由选择，自治系统之间的路由选择称为域间路由选择。

(2) 路由选择协议分为两大类：内部网关协议(IGP)、外部网关协议(EGP)。

(3) 内部网关协议是在一个自治系统内部使用的路由选择协议，这与 Internet 中的其他自治系统选用什么路由选择协议无关。目前，内部网关协议主要有路由信息协议(RIP)和开放最短路径优先(OSPF)协议等。

(4) 若源主机和目的主机处在不同的自治系统中,并且这两个自治系统使用不同的内部网关协议,那么当分组传送到一个自治系统的边界时,就需要使用一种协议将路由选择信息传递到另一个自治系统中,这时需要使用外部网关协议。外部网关协议主要是边界网关协议 BGP。

从以上分析中可以看出,D 的描述是错误的。

答案:D。

5-4-18 分析:设计这道例题的目的是加深读者对 RIP 与距离向量路由选择概念的理解。在讨论 RIP 与距离向量路由选择时,需要注意以下几个主要问题:

关于 RIP 与距离向量路由选择的理解需要注意以下几个基本问题。

(1) 内部网关协议 RIP 是基于距离-向量路由选择算法的。

(2) RIP 要求路由器都要维护从它到每个内部路由器的距离向量。

(3) RIP 定义的距离有几点说明:

① 距离也称为跳数。

② 与路由器直接连接的网络的距离值为 1。

③ 每经过一个路由器,距离值加 1。

④ 距离或跳数最大为 15。

(4) RIP 协议有以下特点:

① 只与相邻路由器交换路由信息。

② 路由器交换的信息是当前最新的路由表。

③ 按照规定的时间间隔交换路由信息。

④ 路由表更新的原则是找出到达每个网络的最短距离。

(5) 在使用 RIP 协议的自治系统中,每个路由器刚开始时只知道直接与它连接的网络距离。接着通过与相邻路由器交换路由信息的过程,路由表逐渐增大,逐步覆盖到达内部网络各个节点的全部路径,并处于不断地更新过程中。

基于以上的知识可以判断,C 的描述是错误的。

答案:C。

5-4-19 分析:设计这道习题的目的是帮助读者深入理解 RIP 协议。RIP 协议限定路径的最大距离值为 16,即允许的最大跳数是 15。因此,路由器 R1 收到邻居节点路由器 R2 的距离向量中包括信息〈net1,16〉,表示 R1 不能经过 R2 到达 net1。

答案:D。

5-4-20 分析:设计这道例题的目的是加深读者对 OSPF 协议概念和特征的理解。在讨论 OSPF 协议概念和特征时,需要注意以下几个主要问题:

(1) 图 5-24 给出一个典型的自治系统的结构示意图。

(2) OSPF 协议可以将一个自治系统分成两级的区域,即主干区域与区域。主干区域为一级域,而其他区域为二级域。每个区域有一个区域标识符,主干区域标识符为 0。

(3) 自治系统中有 4 类路由器:区域内部路由器、主干路由器、区域边界路由器与 AS 边界路由器。主干路由器可以同时是区域边界路由器。

因此,B 的描述是错误的。

答案:B。

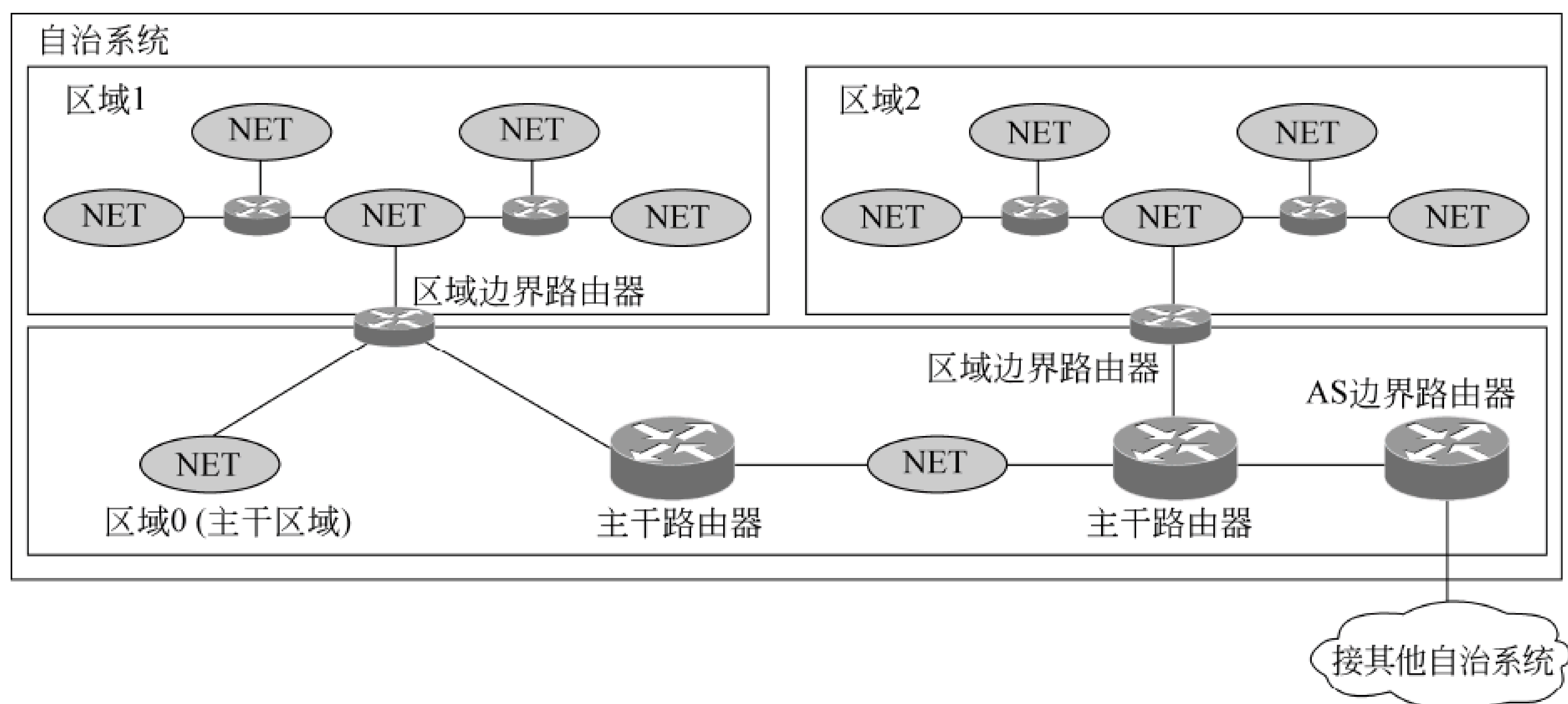


图 5-24　一个典型的自治系统的结构示意图

5-4-21　分析：设计这道例题的目的是加深读者对 OSPF 协议工作过程与链路状态协议的理解。在讨论 OSPF 协议工作过程与链路状态协议时，需要注意以下几个主要问题：

(1) OSPF 使用链路状态协议来实现 AS 内部路由表的更新。

(2) 链路状态协议与距离-向量协议的区别主要表现在以下 3 点：

① 距离-向量协议要求每个路由器与它相邻的路由器交换路由信息；而链路状态协议要求每个路由器用洪泛方法，向 AS 中其他的路由器发送路由信息。

② 距离-向量协议要求路由器向相邻的路由器发送最新的路由表；而链路状态协议要求路由器发送的路由信息包括这个路由器的部分"链路状态"，即与该路由器相邻的路由器是哪些，以及该链路的"度量"。OSPF 的链路度量可以是距离、带宽、延时、费用等。

③ 距离-向量协议要求路由器定时与相邻路由器交换路由信息；而链路状态协议要求在链路状态发生变化时才向 AS 中的其他路由器发送路由信息。

(3) 距离-向量协议与链路状态协议都是在寻找一条"最短"的路径。

从以上讨论中可以看出，C 的描述是错误的。

答案：C。

5-4-22　分析：设计这道例题的目的是加深读者对 BGP 协议概念和特征的理解。关于 BGP 协议特征的理解需要注意以下几个问题：

(1) 在一个自治系统内部一般推荐使用 OSPF 路由协议，而在自治系统之间可以使用 BGP 路由选择协议。BGP 的路由选择算法是基于路径向量路由选择算法。

(2) BGP 的路径向量(path vector)算法与距离-向量(distance vector)、链路状态(link state)算法都不相同，执行 BGP 协议路由器的路由表包括分组到达目的网络的路径。

(3) BGP 要求相邻的 AS 边界路由器之间要交换到达目的网络的路径。

(4) BGP 要求相邻的 AS 边界路由器之间要在规定的时间间隔(如 30s)交换路由信息。

从以上讨论中可以看出，D 的描述是错误的。

答案：D。

5-4-23　分析：设计这道习题的目的是帮助读者进一步了解 3 种路由协议的区别。

(1) RIP 协议是用 UDP 报文封装。UDP 的熟知端口号 520 表示报文封装的是 RIP

数据。

(2) OSPF 协议是用 IP 分组封装。IP 分组结构的“协议”字段中数值 89 表示分组封装的是 OSPF 数据。

(3) BGP 协议的报文是用 TCP 报文封装。TCP 的熟知端口号 179 表示报文封装的是 BGP 数据。

*5-4-24** 设计这道习题的目的是帮助读者进一步了解 3 种路由协议在路由表更新方面的区别。

(1) RIP 协议。

① RIP 协议规定路由器设置一个周期更新定时器，每隔 30s 在相邻路由器之间交换一次路由更新信息。

② 为每个路由表项增加一个超时定时器，在路由表中一项记录被修改之时开始计时，当该项记录在 180s(相当于 6 个 RIP 刷新周期)没有收到刷新信时，表示该路径已经出现故障，路由表将该项记录置为“无效”，而不是立即删除该项路由记录。

③ RIP 协议另外设置了一个清除定时器。如果路由表的一项路由记录置为“无效”后超过 120s 没收到更新信息，则立即从路由表中删除该项记录。

(2) OSPF 协议。

OSPF 的路由器每隔 30 分钟，用洪泛法向所有路由器广播链路状态信息，建立并维护一个区域内同步的链路状态数据库。

(3) BGP 协议。

① 两个 BGP 发言人的相邻关系就建立。一旦 BGP 连接关系建立，就要设法维持这种关系。双方中的每方都需要确信对方是存在的，并且一直在保持这种相邻关系。因此，这两个 BGP 发言人彼此要周期性(通常是每隔 30s)交换“保活分组”。

② BGP 发言人可以用“更新分组”撤销它以前曾经通知过的路由，也可以宣布增加新的路由。撤销路由时可以一次撤销很多条，但增加路由时每次只能增加一条。当某个路由器或链路出现故障时，由于 BGP 发言人可以从不止一个相邻边界路由器获得路由信息，因此很容易选择出新的路由。

5.5 互联网控制报文协议 ICMP

5-5-1 分析：设计该例题的目的是检查读者对 ICMP 协议的产生背景、作用和特点掌握的情况。在讨论 ICMP 协议时，需要注意以下几个主要问题：

(1) IP 协议提供了一种无连接、尽力而为的服务。IP 协议的优点是简洁，它的缺点是缺少差错控制和查询机制。ICMP 就是为了解决以上问题而设计的。ICMP 的差错与查询、控制功能对于保证 IP 协议的可靠运行是至关重要的。

(2) ICMP 本身是网络层的一个协议，但是它的报文不是直接传送给数据链路层，而是要封装成 IP 数据报，然后再传送给数据链路层。从这一点来说，它在层次上高于 IP 协议。但是从协议体系上看，ICMP 的差错和控制信息传输只是要解决 IP 协议可能出现的不可靠问题，它不能独立于 IP 协议而单独存在，因此应该把它视为 IP 协议的一个部分，而归于 IP 协议的体系。

(3) ICMP 差错报告采用路由器-源主机的模式，路由器在发现数据报传输出现错误时

只向源主机报告差错原因。

(4) ICMP 报文类型可以分为两类：差错报告报文和查询报文。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

5-5-2 分析：设计这道习题的目的是帮助读者加深对 ICMP 协议特点的理解。

ICMP 协议的特点主要表现在以下几个方面：

(1) ICMP 本身是网络层的一个协议，但是它的报文不是直接传送给数据链路层，而是要封装成 IP 分组，然后再传送给数据链路层。

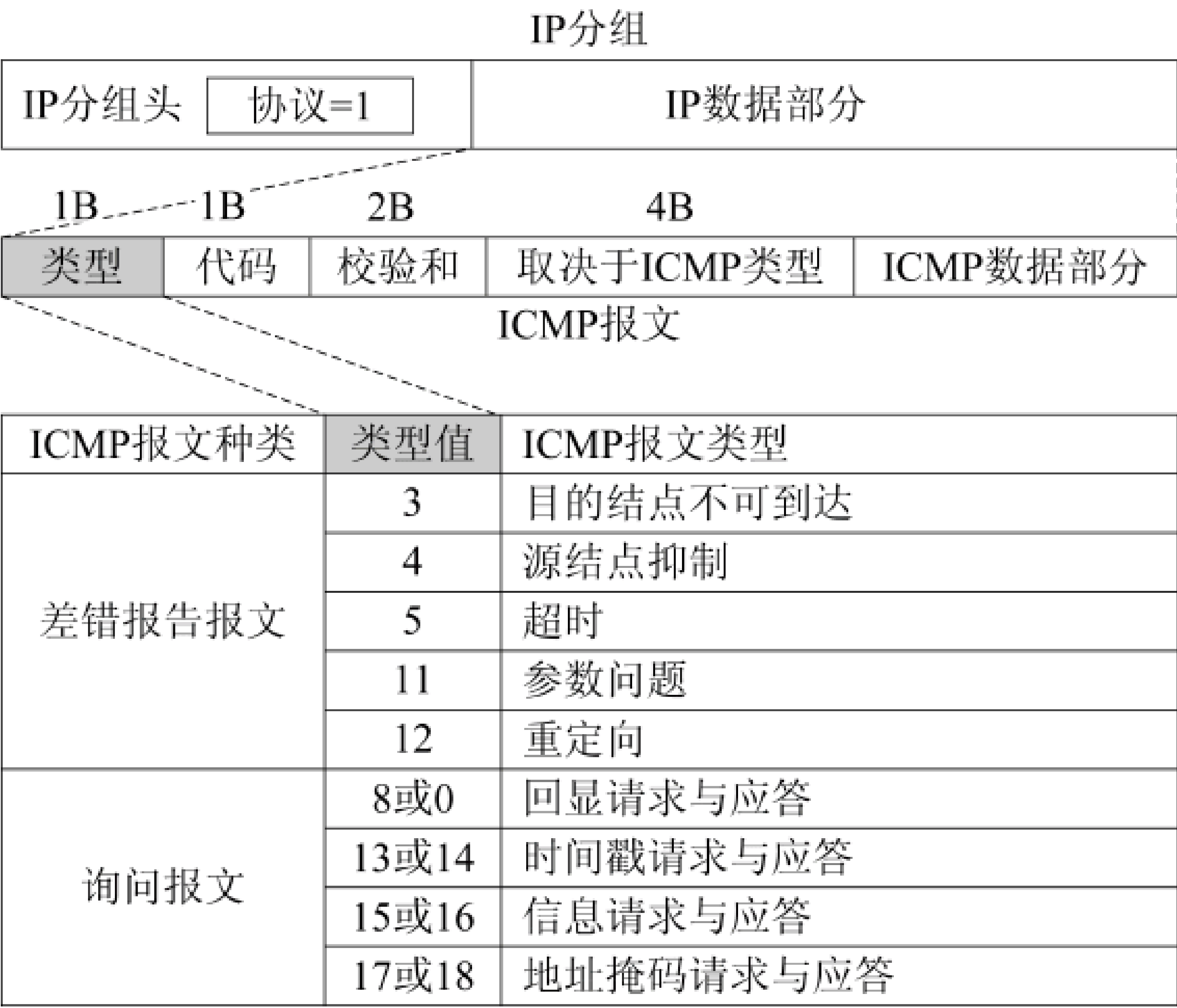
(2) 从协议体系上看，ICMP 只是要解决 IP 协议可能出现的不可靠问题，不能独立于 IP 协议而单独存在，它是 IP 协议的一个组成部分。

(3) ICMP 设计的初衷是用于 IP 协议在执行过程中的出错报告，严格地说，是由路由器向源主机报告传输出错的原因。差错处理需要由高层协议完成。

因此，A 的描述是错误的。

答案：A。

5-5-3 分析：图 5-25 为 ICMP 报文结构示意图。理解 ICMP 报文结构，需要注意以下几个问题：



ICMP报文种类	类型值	ICMP报文类型
差错报告报文	3	目的结点不可到达
	4	源结点抑制
	5	超时
	11	参数问题
	12	重定向
询问报文	8或0	回显请求与应答
	13或14	时间戳请求与应答
	15或16	信息请求与应答
	17或18	地址掩码请求与应答

图 5-25 ICMP 报文结构示意图

(1) 在 IP 分组头中，协议字段值为 1 表示 IP 分组的数据部分是 ICMP 报文。

(2) ICMP 报文的前 4B 的格式是统一的，第一个字段(1B)是类型，第二个字段(1B)是代码，第三个字段(2B)是校验和。第四个字段(4B)的内容与类型相关。在这四个字段之后是数据字段。

(3) ICMP 报文分为两类：差错报告报文与询问报文。不同的差错报告报文对应不同的类型值，例如目的主机不可到达的类型值为 3。询问报文应该是一方请求，另一方应答，因此类型值应该是两个，例如回送请求报文的类型值为 8，回送应答报文的类型值为 0。

(4) IP 分组只对分组头进行校验，而不包括分组数据，而 ICMP 报文是封装在 IP 数据

字段中。为了保证ICMP报文传输的正确性，在ICMP报头中有2B的校验字段。

因此，A关于IP分组头中协议字段值与ICMP报文关系的描述是错误的。

答案：A。

5-5-4 分析：设计这道习题的目的是帮助读者理清ICMP差错报文之间容易混淆的部分。

ICMP差错报文主要有5类：目的主机不可达、源主机抑制、超时、参数问题和重定向。其中，目的不可达、源主机抑制与超时报文容易混淆。

(1)“目的不可达”报文主要有以下7种类型：

- 网络不可达(net unreachable)。
- 主机不可达(host unreachable)。
- 协议不可达(protocol unreachable)。
- 端口不可到达(port unreachable)。
- 源路由选择不能完成(source route failed)。
- 目的网络不可知(unknown destination network)。
- 目的主机不可知(unknown destination host)。

(2) 源主机抑制(source quench)。

路由器出现拥塞的原因主要是处理速度慢，接收的分组数量多于转发分组的数量，当等待处理的分组过多，路由器缓冲区空间不足，必然要造成路由器的拥塞。“源抑制”是当路由器或主机因拥塞而丢弃一个分组时，就向源主机发送源抑制报文。

(3) 超时。

ICMP超时报文是为防止路由表出现问题，造成分组在某些路由器之间无休止的传输而设置。

答案：B。

5-5-5 分析：设计这道题的目的是帮助读者掌握ICMP报文不同类型的“目的不可达”的特点。

(1) 目的不可达是指：路由器寻址出错，下一跳路由器可能存在故障。网络不可达报文只能由路由器产生。

(2) 主机不可达是指：网络寻址不存在问题，可能是目的主机不工作或不存在。这种类型的报文只能由路由器产生。

(3) 协议不可达是指：IP分组携带的数据属于高层协议，如UDP、TCP和OSPF等。如果目的主机收到一个分组的数据字段是TCP协议包，但是目的主机的TCP协议并未运行，这时目的主机不能够处理IP分组传输的TCP数据，主机将产生一个“协议不可达”报文，通知源主机此次传输失败。

(4) 端口不可到达是指：分组要交付的应用进程没有运行。

(5) 目的网络不可知是指：路由器根本不知道关于目的网络的信息。目的网络不可知与网络不可达的区别是：网络不可达是指路由器知道目的主机存在，而无法将分组送达。

(6) 目的主机不可知是指：路由器根本不知道关于目的主机的信息。

因此，C的描述是错误的。

答案：C。

5-5-6 分析：设计这道题的目的是加深读者对ICMP报文“目的不可达”的理解。

(1) 源路由选择不能完成是指：由源主机路由选择选项中规定的一个或多个路由器无法通过。它只能由路由器发送。

(2) 源主机抑制是指：当路由器或主机因拥塞而丢弃一个分组时，就向源主机发送源抑制报文。路由器与主机都可以发送。

(3) 端口不可达是指：分组要交付的应用进程没有运行。它只能由主机发送。

(4) 目的网络不可知是指：路由器根本不知道关于目的网络的信息。目的网络不可知与网络不可到达的区别是：网络不可达是指路由器知道目的主机存在，而无法将分组送达。因此，它也只能由路由器发送。

因此，C的描述是错误的。

答案：C。

5.6 IP多播与IGMP协议

5-6-1 分析：设计该例题的目的是检查读者对多播概念与研究必要性的理解。

(1) 多媒体与实时通信在网络中的应用促进了IP多播技术的发展。

(2) IP多播是指多个接收者可以接收到从同一个或一组源节点一次发送的相同内容的分组。支持多播协议的路由器叫作多播路由器。

(3) IP多播包括以下几个方面内容：

① 定义了一个组地址(group address)。每个组代表了一个(或多个)发送主机与一个(或多个)接收主机之间的一个会话(session)。

② 接收主机可以用多播地址通知多播路由器，该主机希望加入(或退出)哪个多播组。

③ 发送主机使用多播地址发送分组时，不需要了解接收者的位置信息与状态信息。

④ 多播路由器建立一棵从发送主机开始的多播树，这棵树延伸到所有的、其中至少有一个IP多播成员的网络中。利用这棵多播树，多播路由器把多播组的分组一直转发到有多播组成员的网络中。

(4) 支持多播的Internet组管理协议是IGMP协议。

从以上讨论中可以看出，C的描述是错误的。

答案：C。

5-6-2 分析：设计该例题的目的是检查读者对多播主干(MBONE)概念的理解。

(1) 在Internet中，只有一小部分是能够支持多播的多播路由器。某个多播路由器在转发多播分组时可能在邻近找不到其他的多播路由器，这时采用隧道技术是最好的办法。

(2) 两个多播路由器之间如果有多个没有多播功能的普通路由器，则可以利用建立隧道的办法组成多播主干。

(3) 建立隧道的办法是将多播分组封装在单播分组中，将多播分组变成单播分组的数据部分(有效载荷)。这些单播路由器按照单播分组来转发多播分组，直至下一个多播路由器。对于隧道两端的多播路由器来说，组成隧道的单播路由器好像并不存在。

从以上讨论中可以看出，D的描述是错误的。

答案：D。

5-6-3 分析：设计该例题的目的是加深读者对IP多播地址的理解。在讨论IP多播地

址时，需要注意以下几个主要问题：

(1) D类 IP 地址可以用于多播地址。D类 IP 地址的范围在 224.0.0.0～224.255.255.255。D类 IP 地址可以用于标识 2^{28} 个多播组。

(2) 多播地址只能够用于目的地址，而不能够用于源地址。

(3) IP 多播协议支持两类多播地址：永久组地址与临时组地址。

(4) IANA 指派的永久多播组地址，例如：

224.0.0.1　本网所有参加多播的主机与路由器

224.0.0.2　本网所有参加多播的路由器

224.0.0.5　本网所有参加多播的 OSPF 路由器

……

224.0.1.0～238.255.255.255　全球范围都可以使用的多播地址

239.0.0.0～239.255.255.255　限制在一个组织中使用的多播地址

从以上分析中可以看出，B 的描述是错误的。

答案：B。

5-6-4　分析：设计该例题的目的是检查读者对多播路由选择基本概念的理解。

(1) 为了有效地进行多播，需要建立一个由源节点为根，组成员为树叶的支撑树。支撑树从根到树叶的每个路径都是可能的最短路径。

(2) 多播协议在多播时使用两种类型的树：组共享树与源端基准树。

(3) 在使用组共享树方法时，系统中有 N 个组，那么最多有 N 个树。

(4) 在使用源端基准树方法时，源端与组的组合决定了树的结构。

从以上分析中可以看出，B 的描述是错误的。

答案：B。

5.7　MPLS 协议

5-7-1　分析：设计该例题的目的是加深读者对拥塞控制概念的理解。在讨论拥塞控制概念时，需要注意以下几个主要问题：

(1) 当一个子网或子网的一部分出现过多的分组，造成网络性能的下降，这种现象称为拥塞。

(2) 拥塞控制与流量控制的区别：

① 拥塞控制的任务是确保子网能够承受所有到达的分组流量。因此，拥塞控制是一个全局性的问题。造成拥塞的原因涉及网络的各个方面，包括所有的主机、路由器、信道带宽，以及主机与路由器的带宽、内存和处理能力等。

② 流量控制与特定的发送方和接收方之间的点-点流量相关，研究的是局部性的问题。如果点-点通信的发送方发送的流量超过了接收方处理分组的能力，势必造成接收方不能够及时处理进入的分组，等待队列过长，一旦超出队列最大长度，最终会造成缓冲区溢出而丢弃分组。

(3) 拥塞控制的实现需要解决 3 个基本问题：如何发现网络出现拥塞，如何通过拥塞控制算法产生解决方案，如何将控制信息传送给执行节点。

(4) 拥塞控制算法可以分为开环算法与闭环算法。闭环算法又可以进一步分为显式反

馈与隐式反馈。显式反馈算法采取从拥塞节点向源节点发送分组,报告拥塞出现。隐式反馈算法由源节点通过检测如确认分组达到时间的方法,来判断是否出现拥塞。

(5) 拥塞解决方法主要有增加资源与减小负荷。

从以上分析中可以看出,D的描述是错误的。

答案:D。

5-7-2 分析:设计该例题的目的是加深读者对QoS概念的理解。在讨论QoS概念时,需要注意以下几个主要问题:

(1) 网络中从源节点到目的节点的分组流(stream)称为一个流(flow)。

(2) 一个流所要求的服务质量QoS可以用4个参数表述:可靠性、延时、延时抖动与带宽。

(3) 解决IP协议QoS问题的主要方法:综合服务IntServ、资源预留协议RSVP、区分服务DiffServ与多协议标记服务MPLS。

(4) 资源预留协议RSVP由源节点通过向目的节点预留资源的方法来保证IP分组传输的服务质量。

(5) 区分服务DiffServ通过服务等级协定(SLA)将服务类型按要求的吞吐率、分组丢失率、延时、延时抖动与网络可用性来分级,对不同等级的服务提供不同网络资源,以保证IP分组传输的服务质量。

(6) 多协议标记服务MPLS的改进表现在:在IP网络中提供一种面向连接的服务;动态定义路由,优化网络利用率的能力;支持VPN;支持多种网络层协议。

从以上分析中可以看出,C的描述是错误的。

答案:C。

5.8 地址解析协议

5-8-1 分析:设计该例题的目的是加深读者对地址解析协议(ARP)概念的理解。在讨论ARP概念时,需要注意以下几个主要问题:

(1) 对于TCP/IP协议来说,主机和路由器在网络层用IP地址来标识,在数据链路层用物理地址(例如Ethernet的MAC地址)来标识。

(2) 在描述一个网络的工作过程时,实际上是做了一个假设:已经知道通信的目的主机的IP地址,并且知道对应这个IP地址的物理地址。这个假设成立的条件是:在任何一台主机或路由器中必须有一张“IP地址-物理地址对照表”,它应该包括你需要通信的一台主机或路由器的信息。

(3) 通过“静态映射”的方法,从一个已知的IP地址获取对应的物理地址。但是,这是非常理想的一种解决方案,在一个小型的互联网络系统中实现比较容易,这在大型网络中几乎是不可能实现的。因此,在Internet中必须设计一种“动态映射”的方法,以解决IP地址与MAC地址映射的问题。

(4) 从已知的IP地址找出对应的MAC地址的映射过程称为正向地址解析,相应的协议称为地址解析协议(ARP)。从已知的MAC地址找出对应的IP地址的映射过程称为反向地址解析,相应的协议叫作反向地址解析协议(RARP)。

从以上分析中可以看出,D关于ARP特征的描述是错误的。

答案：D。

5-8-2 分析：设计这道习题的目的是帮助读者加深对 ARP 协议的认识。

数据链路层 MAC 地址、网络层 IP 地址、传输层端口号与应用层域名容易混淆。ARP 是网络层协议，它的功能是根据 IP 地址查询对应节点网卡的 MAC 地址。因此，A 的描述是正确的。

答案：A。

5-8-3 分析：设计该例题的目的是加深读者对 ARP 协议的理解。在讨论 ARP 协议时，需要注意以下几个主要问题：

（1）在 TCP/IP 协议中，从已知的 IP 地址找出对应 MAC 地址的映射过程叫作正向地址解析，相应的协议叫作地址解析协议（ARP）。从已知的 MAC 地址找出对应 IP 地址的映射过程叫作反向地址解析，相应的协议叫作反向地址解析协议（RARP）。

（2）地址解析的基本工作过程如下：

① 在发送一个分组之前，首先根据目的 IP 地址，在本地 ARP 高速缓存表中查找与之对应的目的 MAC 地址。如果可以找到，则不进行地址解析。如果查找不到，则需要进行地址解析。

② 实现地址解析的第一步是产生 ARP 请求分组，在相应的字段写入本地主机的源 MAC 地址与源 IP 地址、目的 IP 地址，而在目的 MAC 地址字段写入 0。

③ 将 ARP 分组传送到本地的数据链路层，并组装成帧。以源 MAC 地址作为源地址，以广播地址作为目的地址发送出去。

④ 目的主机识别该 IP 地址，接收该分组。

⑤ 完成地址解析的目的主机发送 ARP 应答分组，该分组包括对方需要知道的目的 MAC 地址。

⑥ 源节点接收到 ARP 应答分组，知道对应于目的 IP 地址的目的 MAC 地址，将它作为一条新的记录，加入到 ARP 高速缓存表。

⑦ 源节点将有完整的源 IP 地址、源 MAC 地址、目的 IP 地址、目的 MAC 地址信息和数据作为一个发送分组，传送给它的数据链路层并封装成帧，然后以点对点方式发送到目的主机。

（3）改进地址解析方法可以采用高速缓存、代理 ARP 技术等方法。

从以上分析中可以看出，A 的描述是错误的。

答案：A。

* **5-8-4** 分析：设计这道习题的目的是帮助读者深入地理解 ARP 协议的工作原理。

（1）ARP 请求分组。

ARP 分组结构如图 5-26 所示。

根据 ARP 协议的规定，

- 硬件类型是指：硬件地址类型，这里是指 Ethernet，十六进制数值为 0x01。
- 协议类型是指：映射的协议地址类型，这里是指 IPv4，十六进制数值为 0x0800。
- 硬件地址长度：MAC 地址长度，6B，对应字段的十六进制数值为 0x06。
- 协议地址长度：IP 地址长度，4B，对应字段的十六进制数值为 0x04。
- 操作类型：ARP 请求值为 1，ARP 应答值为 2，RARP 请求值为 3，RARP 应答值为 4。
- 源 MAC 地址：发出 ARP 请求报文的主机 MAC 地址 23-45-AB-4F-67-CD。

<table>
<tr><td colspan="2">硬件类型</td><td>协议类型</td></tr>
<tr><td>硬件地址长度</td><td>协议地址长度</td><td>操作类型</td></tr>
<tr><td colspan="3">源MAC地址</td></tr>
<tr><td colspan="2">源MAC地址</td><td>源IP地址</td></tr>
<tr><td colspan="2">源IP地址</td><td>目的IP地址(全0)</td></tr>
<tr><td colspan="3">目的MAC地址(全0)</td></tr>
<tr><td colspan="3">目的IP地址</td></tr>
</table>

图 5-26 ARP 分组结构示意图

- 源 IP 地址：发出 ARP 请求报文的主机 IP 地址 125.45.23.12，转化成十六进制表示为 7D2D170CH。
- 目的 MAC 地址：ARP 请求报文的目的 MAC 地址是全 0。
- 目的 IP 地址：ARP 服务器的 IP 地址为 125.11.78.10，转化成十六进制表示为 7D0B4E0AH。

主机发出 ARP 的请求报文为：

<table>
<tr><td colspan="2">0x01</td><td>0x0800</td></tr>
<tr><td>0x06</td><td>0x04</td><td>0x01</td></tr>
<tr><td colspan="3">0x2345AB4F</td></tr>
<tr><td colspan="2">0x67CD</td><td>0x7D2D(125.45)</td></tr>
<tr><td colspan="2">0x170C (23.12)</td><td>0x0000</td></tr>
<tr><td colspan="3">0x00000000</td></tr>
<tr><td colspan="3">7D0B4E0A(125.11.78.10)</td></tr>
</table>

(2) 如果目的主机的 MAC 地址为 AA-BB-BA-A2-4F-68-09。试给出 ARP 响应分组各项的数据。

需要注意的是，ARP 请求报文是主机发送给 ARP 服务器，而应答报文是 ARP 服务器发送给主机的，源与目的正好相反。

服务器发出 ARP 的应答报文为：

<table>
<tr><td colspan="2">0x01</td><td>0x0800</td></tr>
<tr><td>0x06</td><td>0x04</td><td>0x02</td></tr>
<tr><td colspan="3">0xAABBBAA24F</td></tr>
<tr><td colspan="2">0x6809</td><td>0x7D0B(125.11)</td></tr>
<tr><td colspan="2">0x4E0A (78.10)</td><td>0x2345</td></tr>
<tr><td colspan="3">0xAB4F67CD</td></tr>
<tr><td colspan="3">7D0B170C(125.45.23.12)</td></tr>
</table>

(3) 将问题(1)的结果封装成数据链路层的帧。Ethernet 帧结构如图 5-27 所示。

SFD	目的地址	源地址	类型	数据	FCS
8B	6B	6B	2B	46~1500B	4B

图 5-27 Ethernet 帧结构示意图

在将ARP的请求报文封装成Ethernet帧时，需要注意的就是，ARP的请求报文的数值一般是用十六进制数来表示，而Ethernet帧的数值一般是用二进制数来表示。其中，MAC地址已经用十六进制数表示，那么需要将前导码SFD与类型字段值用十六进制表示。

前导码SFD用二进制数表示是31个“10”与1个“11”组成，转化成十六进制数时分割成14个“1010”与1个“1011”，可以14个“A”与1个“AB”表示，即0xAAAAAAAAAAAAAAAB。

类型字段2B，ARP报文的值为0x0806。

封装成Ethernet帧的ARP请求报文结构如图5-28所示。

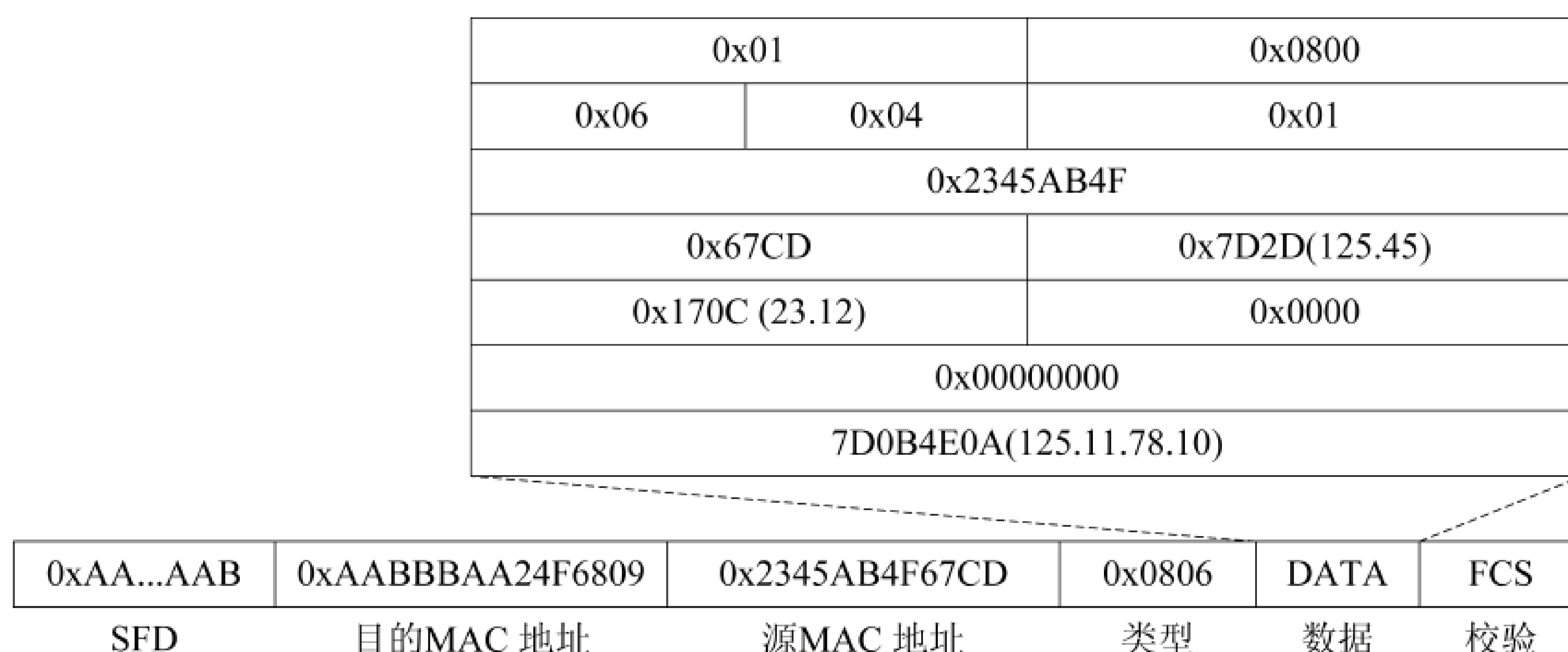


图5-28 封装成Ethernet帧的ARP请求报文结构示意图

(4) 将问题(1)的结果封装成数据链路层的帧。

封装成Ethernet帧的ARP应答报文结构如图5-29所示。这里，只需要将帧中源MAC地址与目的MAC地址对换即可。

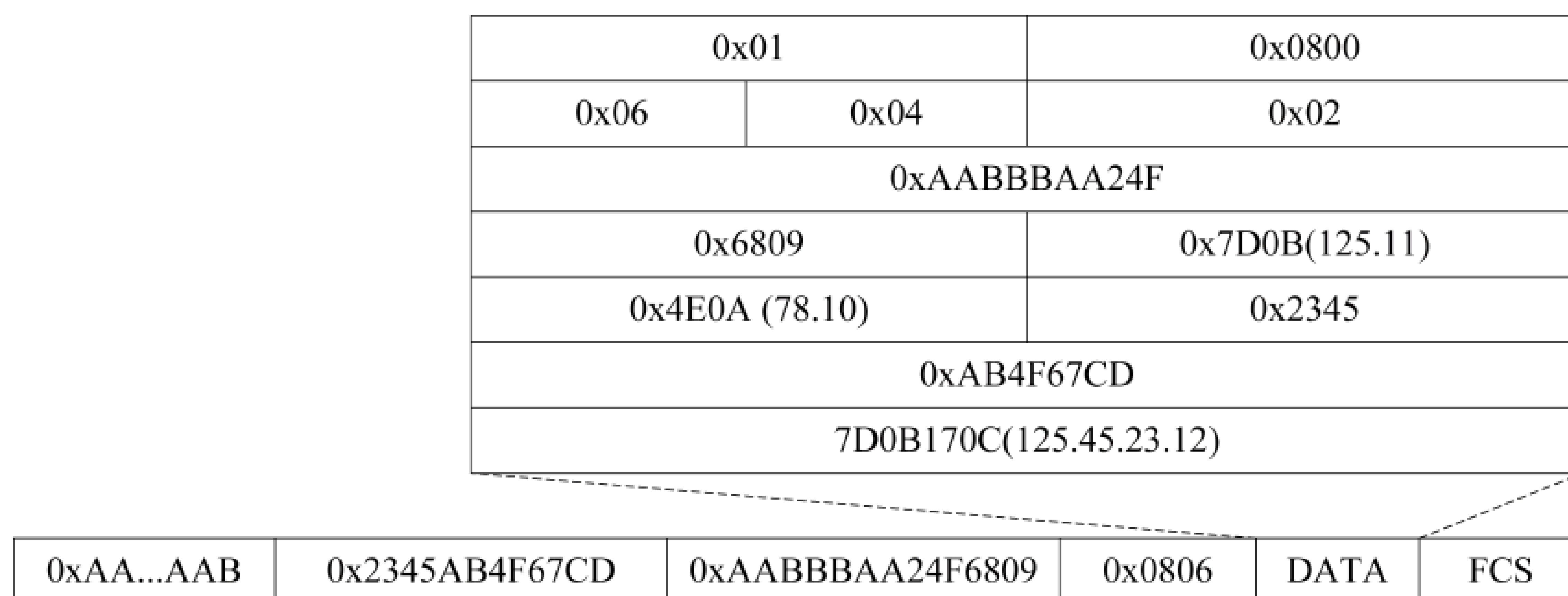


图5-29 封装成Ethernet帧的ARP应答报文结构示意图

5.9 移动IP协议

5-9-1 分析：设计该例题的目的是加深读者对移动IP基本术语的理解。在讨论移动IP基本术语时，需要注意以下几个主要问题：

(1) 家乡地址是指家乡网络为每个移动节点分配的一个长期有效的IP地址。转交地址是指当移动节点接入一个外地网络时，被分配的一个临时的IP地址。家乡网络是指为移

动节点分配长期有效的IP地址的网络。目的地址为家乡地址的IP分组,将会以标准的IP路由机制发送到家乡网络。

(2) 家乡链路是指移动节点在家乡网络时接入的本地链路。外地链路是指移动节点在访问外地网络时接入的链路。家乡链路与外地链路能够比家乡网络与外地网络更精确地表示出移动节点所接入的位置。

(3) 移动绑定是指家乡网络维护移动节点的家乡地址与转发地址的关联。

(4) 在移动IP中,家乡代理通过隧道将发送给移动节点的IP分组转发到移动节点。隧道的一端是家乡代理,另一端一般是外地代理,也有可能是移动节点。

从以上分析中可以看出,B对转交地址的描述是错误的。

答案:B。

5-9-2 分析:设计该例题的目的是加深读者对移动IPv4工作原理的理解。在讨论移动IPv4基本工作原理时,需要注意以下几个主要问题:

(1) 移动IPv4的工作过程可以分为4个阶段,即代理发现、注册、分组路由与注销。

(2) 移动IPv4代理发现是通过扩展ICMP路由发现机制来实现。它定义了"代理通告"和"代理请求"两种新的报文,用于判断节点是否从一个网络切换到另一个网络,是在家乡网络还是在外地网络。

(3) 移动节点到达新的网络后,通过注册过程把自己新的可达信息通知家乡代理。移动IPv4为移动节点到家乡代理的注册定义了两种不同的过程:一种过程是通过外地代理转发移动节点的注册请求,另一种过程是移动节点直接到家乡代理上进行注册请求。

(4) 移动IP的分组路由可以分为单播、广播与多播。

(5) 如果移动节点已经回到家乡网络,那么它需要到家乡代理进行注销。

从以上分析中可以看出,移动IPv4代理发现是通过扩展ICMP路由发现机制来实现。"代理通告"和"代理请求"是两种新的ICMP报文。因此,B的描述是错误的。

答案:B。

5.10 IPv6 协议

5-10-1 分析:设计该例题的目的是检查读者对IPv6与IPv4报头结构的掌握情况。

IPv6与IPv4报头的差异主要表现在以下几点:

(1) IPv6报头字段的数量从IPv4的12个(包括选项)减少到8个,并且IPv6报头长度是固定的,IPv4报头长度是可变的。因此,IPv6报头可以取消"报头长度"字段。

(2) IPv6中间路由器必须处理的字段数从IPv4的6个减少到4个,路由器可以更有效率地转发IPv6数据包。

(3) IPv6有效载荷长度字段取代了IPv4的总长度字段。IPv4的总长度包括报头长度,而IPv6只表示有效载荷的长度。

(4) IPv6地址长度是IPv4地址长度的4倍,而IPv6报头长度是IPv4最小报头长度的两倍。

(5) IPv6通信类型字段取代了IPv4服务类型字段。

(6) IPv6跳步限制字段取代了IPv4生存时间字段。

(7) IPv6将IPv4报头中的支持拆分的字段(如标识、标志、片偏移项)移到扩展报头中。

(8) IPv6 的下一个报头字段取代 IPv4 报头中的协议字段。

(9) IPv6 取消了报头校验和字段,相应的功能由数据链路层承担。

(10) IPv6 取消了报头选项字段,用扩展报头中取代 IPv4 报头中的选项字段。

答案:B。

5-10-2 分析:设计该例题的目的是检查读者对 IPv4 到 IPv6 过渡方法的理解。

(1) IPv4 到 IPv6 过渡方法可以分为双 IP 协议层、双协议栈、隧道技术等。

(2) 双 IP 协议层与双协议栈方案是不同的。双协议栈是指一个节点同时运行 IPv4 与 TCP/UDP,以及 IPv6 与 TCP/UDP,它不仅包括网络层,也包括传输层。

(3) 隧道配置可以分为 3 种类型:路由器-路由器、主机-路由器或路由器-主机,以及主机-主机。

答案:A。

5-10-3 分析:

关于 IPv6 地址表示方法的规定中需要注意以下几个基本问题:

(1) IPv6 的 128 位地址按每 16 位划分为一个位段,每个位段被转换为一个 4 位的十六进制数,并用冒号":"隔开,这种表示法称为冒号十六进制表示法。

(2) 有些 IPv6 地址中可能包含一长串 0。为了进一步简化 IP 地址表达,如果几个连续位段的值都为 0,那么这些 0 就可以简写为::,称为双冒号表示法。

(3) 在使用零压缩法时,不能将一个位段内部的有效 0 压缩掉。

(4) ::双冒号在一个地址中只能出现一次。

基于上述原则,C 中出现了两个"::",违反第(4)条的规定。

答案:C。

5-10-4 分析:

确定::之间表示被压缩了多少位 0,可以数一下地址中还有多少个位段,然后用 8 减去这个数,再将结果乘以 16。

计算:

该地址有 4 个位段,因此结果为(8−4)×16=64。

答案:::之间被压缩了 64 位 0。

第三部分　综合练习——术语解析

从给出的 26 个定义中挑出 20 个,并将标识定义的字母填在对应术语前的空格位置。

(1) ________ ARP　　(2) ________分组总长度

(3) ________专用地址　　(4) ________严格源路由

(5) ________ CIDR　　(6) ________ MPLS

(7) ________间接交付　　(8) ________直接广播地址

(9) ________移动 IP　　(10) ________分组头长度

(11) ________扩展报头　　(12) ________松散源路由

(13) ________ ICMP　　(14) ________特定主机地址

(15) ________ TTL 字段　　(16) ________路由汇聚

(17) ________ RSVP　　(18) ________路由选择协议

(19) ________受限广播地址　　(20) ________第三层交换路由器

A. IP 分组头中表示网络层 IP 协议版本号的字段。

B. IP 分组头中表示高层协议类型的字段。

C. IP 分组头中 4 位的长度字段。

D. IP 分组头中 16 位的长度字段。

E. IP 分组头中表示转发分组最多经过的路由器跳数的字段。

F. 规定分组经过的路径上每个路由器及顺序的路由。

G. 规定分组一定要经过的路由器,但不是一条完整的传输路径的路由。

H. 标识一台主机、路由器与网络接口的地址。

I. 可以将分组以广播方式发送给特定网络所有主机的地址。

J. 路由器不向外转发,而是将该分组在网络内部以广播方式发送给全部节点的地址。

K. 路由器接到分组不向外转发该分组,而是直接交付给本网络中指定主机的地址。

L. 只能够用于内部网络,而不能够在 Internet 进行路由的地址。

M. 将 IP 地址按可变大小的地址块来分配的方法。

N. 目的主机与源主机不在同一网络的分组转发方法。

O. 路由器中用来产生路由表的算法。

P. 用于实现路由表中路由信息动态更新的方法。

Q. 用来减少路由表中路由项数量的方法。

R. 有权自主决定内部所采用的路由选择协议的单元。

S. 将第三层路由技术与第二层硬件交换技术相结合的网络互联设备。

T. 具有差错与查询、控制功能的网络层协议。

U. 源节点和目的节点之间在会话之前建立一个连接,预留所需资源的协议。

V. 路由使用第三层的路由协议,而交换是用第二层硬件去完成的协议。

W. 实现 IP 地址与 MAC 地址映射功能的协议。

X. 能够帮助移动节点在改变接入点时保持通信连续性的技术。

Y. 长度为 128 位地址的网络层地址。

Z. IPv6 报头的下一个报头字段指向的位置。

参考答案:

(1) W　(2) D　(3) L　(4) F　(5) M

(6) V　(7) N　(8) I　(9) X　(10) C

(11) Z　(12) G　(13) T　(14) K　(15) E

(16) Q　(17) U　(18) P　(19) J　(20) S

第 6 章 传输层

第一部分　同 步 练 习

6.1　传输层的基本概念

6-1-1　以下关于传输层基本概念的描述中，错误的是________。

A. 网络层解决由“点-点”链路组成的传输路径的路由选择与分组交付问题

B. 传输层在源主机与目的主机的应用进程之间建立“端-端”连接

C. 设计传输层的目的就是为了改善传输网络的性能

D. TPDU 头用于传达传输层协议的命令和响应

6-1-2　以下关于应用进程、传输层接口与套接字的描述中，错误的是________。

A. 应用进程是在应用程序开发者控制下工作，它不依赖于主机操作系统

B. 一个 IP 地址与一个进程标识称为一个“套接字”或“套接字地址”

C. 传输层的 TCP 或 UDP 协议是在主机操作系统控制下工作

D. 套接字也叫作应用程序编程接口 API

6-1-3　以下关于网络环境中应用进程标识的描述中，错误的是________。

A. IANA 定义的端口号有熟知端口号、注册端口号和临时端口号

B. 客户程序使用的临时端口号数值范围为 49152～65535

C. 服务器程序分配的熟知端口号值的范围为 0～1023

D. 传输层协议使用统一的熟知端口号和临时端口号

6-1-4　以下 TCP 熟知端口号中，错误的是________。

A. TELNET：23　　B. SMTP：25　　C. HTTP：80　　D. BGP：161

6-1-5　以下关于 UDP 熟知端口号的描述中，错误的是________。

A. DNS：53　　B. TFTP：67　　C. NTP：123　　D. RPC：111

6-1-6　客户端标识与服务器 TCP 连接的五元组为：TCP，212.10.25.56：1002，121.5.21.2：53。请指出这个五元组标识是正确的还是错误的。为什么？

6.2　UDP 协议

6-2-1　以下关于 UDP 协议主要特点的描述中，错误的是________。

A. UDP 报文的报头长度是可变的
B. 伪报头包括 IP 分组报头的一部分
C. UDP 报头主要包括端口号、长度、检验和等字段
D. UDP 检验和包括伪报头、UDP 报头及应用层数据

6-2-2 以下关于 UDP 协议报文传输特点的描述中,错误的是________。
A. UDP 保留应用程序提交报文的长度与格式
B. UDP 在应用层报文上添加了 UDP 协议头部就向下提交给 IP 层
C. 接收端会将发送端提交传送的报文原封不动地提交给接收端应用程序
D. 为防止应用程序提交的报文太长,UDP 要求应用层提交的 TPDU 长度有限制

6-2-3 假设 UDP 报头的十六进制数为 06 32 00 45 00 1C E2 17。求:
(1) 源端口号与目的端口号。
(2) 用户数据长度。
(3) 这个数据报是客户端发出,还是服务器端发出?
(4) 使用 UDP 协议的服务器是哪种类型?

6-2-4 以下关于 UDP 协议适用范围的描述中,错误的是________。
A. 对数据交付实时性要求较高
B. 对数据交付可靠性要求较高
C. 简单的请求与应答报文的交互
D. 一对一、一对多与多对多的交互式通信

6-2-5 以下关于 UDP 校验和特点的描述中,错误的是________。
A. UDP 校验和的检验范围包括伪头部、UDP 报头与从应用层来的数据
B. 计算校验和时需要在 UDP 用户数据报之前增加 12B 的伪头部
C. 伪头部只在计算时起作用,既不向低层传输,也不向高层传送
D. UDP 长度指 UDP 数据报的长度,包括伪头部的长度

6.3 TCP 协议

6-3-1 以下关于 TCP 协议主要特点的描述中,错误的是________。
A. 支持面向连接与并发的 TCP 连接
B. 确认机制用来检查数据是否安全和完整地到达
C. 允许通信双方的应用程序在任何时候都可以发送数据
D. 支持字节流传输,自动确定接收端应用程序数据字节的起始与终止位置

6-3-2 以下关于 TCP 与 UDP 协议特点的比较中,错误的是________。
A. TCP 提供可靠的报文传输,UDP 提供尽力而为的交付
B. TCP 基于字节流, UDP 基于报文
C. TCP 面向连接,UDP 无连接
D. TCP 传输速率高于 UDP

6-3-3 以下关于 TCP 报头格式的描述中,错误的是________。
A. 报头长度为 20～60B,其中固定部分为 20B
B. 端口号字段分别表示报文段的源端口号与目的端口号

C. 控制字段定义了 8 种用于 TCP 连接、流量控制，以及数据传送的控制位或标志位
D. TCP 校验和伪头部中 IP 分组头的协议字段值为 6

6-3-4 以下关于 TCP 最大段长度的描述中，错误的是________。
A. TCP 协议对报文数据部分最大长度有规定，这个值称为最大段长度 MSS
B. MSS 是 TCP 报文中数据部分的最大字节数限定值，不包括报头长度
C. TCP 报文段的最大长度与窗口最大长度的概念是相同的
D. MSS 的默认值是 536B

6-3-5 主机 A 与主机 B 建立了 TCP 连接。主机 A 向主机 B 连续发送 3 个 TCP 报文段，长度分别为 100B、200B、300B，第一个报文段的序列号为 201，主机 B 在正确接收 3 个报文段之后，发送给主机 A 的确认序列号应该为多少？

6-3-6 一个 TCP 连接要发送 5200B 的数据。第 1 个字节的编号为 10010。如果前 5 个报文段各携带 1000 个字节的数据。请写出每个报文段的序号范围。

6-3-7 根据以下条件，估算 TCP 连接的 RTT 变量值。
已知：收到 3 个连接的确认报文段，它们比相应的数据报文段发送时间分别滞后 26ms、32ms 与 24ms。设：$\alpha=0.9$。

6-3-8 以下关于 TCP 可靠传输的描述中，错误的是________。
A. 确定通信的双方是否存在
B. 分配传输实体可以使用的资源如缓冲区的大小
C. 双方协商通信参数，如最大报文段长度、传输速率
D. TCP 协议的客户与服务器进程之间连接建立要经过“三次握手”

6-3-9 以下关于 TCP 报头中“序号”的描述中，错误的是________。
A. 序号字段长度为 32bit
B. 序号范围在 0～4284967295
C. TCP 发送的字节流中每个字节按顺序编号
D. TCP 连接建立时通信双方要协商一个初始序号

6-3-10 以下关于 TCP 协议最大段长度 MSS 的描述中，错误的是________。
A. MSS 是报文中最大数据长度
B. 默认的 MSS 值为 556B
C. MSS 值可以在建立 TCP 连接时协商
D. TCP 允许连接的双方可以选择不同的 MSS 值

6-3-11 如果 TCP 使用的最大窗口为 64KB，报文段平均往返延时为 20ms。假设传输带宽没有限制，那么 TCP 连接最大的吞吐量是多少？

6-3-12 已知：通信信道带宽为 1Gbps，端-端延时为 10ms，TCP 发送窗口为 65 535B。求：该 TCP 连接可能达到最大的吞吐率，以及信道利用率。

* **6-3-13** 已知：最大报文段长度 MSS＝128B，序号用 8bit 表示，报文段在网络中的生存时间为 30 秒。求：每条 TCP 连接能够达到的最高速率。

* **6-3-14** 已知：TCP 报文段的序号用 64bit 表示。求：如果在光链路上传输，速率为 75Tbps，报文段多长时间不会发生序号重复现象？

* **6-3-15** 已知：一个 TCP 连接使用的是 256kbps 的链路，端-端延时为 128ms，吞吐率为 120kbps。

求：发送窗口为多少？

6-3-16 假设：TCP 拥塞控制的 AIMD 为 2 时，发送端检测出超时，TCP 使用慢开始与拥塞避免。试给出：第 1 次到第 15 次传输的拥塞窗口分别为多少？

6-3-17 TCP 用户数据长度为 8192B，通过 Ethernet 传送。问：是否应该分片？如果需要分片，应该分几个分片？写出每个分片的数据字段长度与片偏移值。

6-3-18 以下关于 TCP 使用的计时器的描述中，错误的是________。

A. 设置重传计时器的目的是控制报文确认与等待重传的时间

B. 设置保持计时器的目的是为了防止 TCP 连接处以长时期空闲

C. 设置时间等待计时器的目的是为了保证 TCP 连接释放过程正常地进行

D. 设置坚持计时器的目的是防止接收端因接收一个长报文的多个分段而造成死锁

6-3-19 主机 A 向主机 B 发送一个建立 TCP 连接的(SYN＝1，seq＝11180)报文段，主机 B 接受连接申请，那么以下 4 个应答报文端中正确是________。

A. (SYN＝0，ACK＝0，seq＝11181，ack＝56421)

B. (SYN＝0，ACK＝1，seq＝56421，ack＝11181)

C. (SYN＝1，ACK＝0，seq＝11181，ack＝56421)

D. (SYN＝1，ACK＝1，seq＝56421，ack＝11181)

6-3-20 主机 A 向主机 B 建立了一个 TCP 连接，主机 A 连续向主机 B 发送了 200B、300B 与 400B 共 3 个报文段。第 3 个报文段的序号是 900。如果主机 B 制正确地接收到第 1 和第 3 个报文段，那么主机 B 向主机 A 发送的确认序号应该是多少？

6-3-21 在 TCP 连接上连续发送 4 个数据长度为 1500B 的报文段，第一个报文段的第一个字节序号为 5001，那么第 3 个报文段的序号范围为________。

A. 1500～6499　　B. 6500～7999　　C. 8001～9500　　D. 9500～1049

* **6-3-22** 下图是 TCP 连接建立的三次握手与连接释放的四次握手过程示意图。请根据 TCP 协议的工作原理，写出图中①～⑧位置的序号值。

Sniffer Portable - Local, Ethernet (Line speed at 100 Mbps) - [a2.cap: Filtered 3, 36/25000 Ethernet Frames, Filter: Matrix]

No	Source Addes	Dest. Addes	Summary	Len(B)
3	202.1.64.166	211.80.20.2	DNS: NAME=www.it.com	77
4	211.80.20.2	202.1.64.166	DNS: IP=201.8.2.2 NAME=www.itnk.com	165
5	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 SYN=1 SEQ=10020	62
6	201.8.2.2	202.1.64.166	TCP: S=80 D=1298 SYN=1 ACK=1 SEQ=25609 ack=①	62
7	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 ACK=1 SEQ=② ack=③	60
8	202.1.64.166	201.8.2.2	HTTP: Port=1535 GET/HTTP/1.1	568

(a) TCP连接建立的三次握手过程

Sniffer Portable - Local, Ethernet (Line speed at 100 Mbps) - [a2.cap: Filtered 3, 36/25000 Ethernet Frames, Filter: Matrix]

No	Source Addes	Dest. Addes	Summarv	Len(B)
	·········			
23	202.1.64.166	201.8.2.2	数据 Len=100 S=1298 D=80 SQL=16651 ack=68830	1080
24	201.8.2.2	202.1.64.166	数据 Len=1005 S=80 D=1298 SQL=68831 ack=16751	165
25	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 FIN=1 SEQ=16955 ack=60036	62
26	201.8.2.2	202.1.64.166	TCP: S=80 D=1298 ACK=1 SEQ=④ ack=⑤	62
27	201.8.2.20	202.1.64.166	TCP: S=80 D=1298 FIN=1 ACK=1 SEQ=⑥ ack=16955	60
28	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 ACK=1 SEQ=⑦ ack=⑧	60

(b) TCP连接释放的四次握手过程

6-3-23 主机 H 通过快速以太网连接到 Internet,IP 地址为 192.168.0.8;服务器 S 的 IP 地址为 211.68.71.80。主机 H 与服务器 S 建立了 TCP 连接。用软件工具捕获的主机 H 的 5 个 IP 分组的前 40B 的内容如下表所示。

编号	IP分组的前40B的内容(十六进制)
1	45 00 00 30 01 9b 40 00 80 06 1d e8 c0 a8 00 08 d3 44 47 50 0b d9 13 88 84 6b 41 c5 00 00 00 00 70 02 43 80 5d b0 00 00
2	45 00 00 30 00 00 40 00 31 06 6e 83 d3 44 47 50 c0 a8 00 08 13 88 0b d9 e0 59 9f ef 84 6b 41 c6 70 12 16 d0 37 e1 00 00
3	45 00 00 28 01 9c 40 00 80 06 1d ef c0 a8 00 08 d3 44 47 50 0b d9 13 88 84 6b 41 c6 e0 59 9f f0 50 10 43 80 2b 32 00 00
4	45 00 00 38 01 9d 40 00 80 06 1d de c0 a8 00 08 d3 44 47 50 0b d9 13 88 84 6b 41 c6 e0 59 9f f0 50 18 43 80 c6 55 00 00
5	45 00 00 28 68 11 40 00 31 06 06 7a d3 44 47 50 c0 a8 00 08 13 88 0b d9 e0 59 9f f0 84 6b 41 d6 50 10 16 d0 57 d2 00 00

根据表中的内容回答以下几个问题:

(1) 5 个分组中,哪几个是由主机 H 发出?哪几个完成了 TCP 连接?哪几个通过快速以太网时进行了填充?

(2) 服务器已经接收到的应用层数据是多少字节?

(3) 如果某个 IP 分组在服务器 S 发出时的前 40B 如下表所示,那么该 IP 分组到达主机 H 时,经过了几个路由器?

S发出的IP分组	45 00 00 28 68 11 40 00 40 06 ec ad d3 44 47 50 ca 76 01 06 13 88 a1 08 e0 59 9f f0 84 6b 41 d6 50 10 16 d0 b7 d6 00 00

6-3-24 用十六进制表示的一个 TCP 报文的头部数据为

0d 28 00 15 00 00 00 06 00 00 00 00 70 02 40 00 c0 29 00 00

回答:

(1) 源端口号与目的端口号各为多少?

(2) 发送序列号是多少?

(3) TCP 头部长度是多少?

(4) TCP 连接是由什么样的应用层协议建立的?

(5) TCP 连接的状态是什么?

第二部分 同步练习答案与解析

6.1 传输层的基本概念

6-1-1 分析:设计该例题的目的是加深读者对传输层基本概念的理解。在讨论传输层的基本概念时,需要注意以下几个主要问题:

(1) 网络层的 IP 地址标识了联网主机、路由器的位置信息;路由算法可以在互联网络

中选择一条由源主机-路由器、路由器-路由器、路由器-目的主机的多段“点-点”链路组成的传输路径,IP 协议通过这条传输路径完成分组数据的传输。

(2) 网络层是传输网络(或承载网)的一部分,而传输网络是由电信公司提供服务的。如果网络层提供的服务不可靠(如频繁丢失分组),用户无法对传输网络加以控制,那么就需要在网络层上再增加一个传输层来改善服务质量。

(3) 传输层协议是要利用网络层所提供的服务,在源主机的应用进程与目的主机的应用进程之间建立“端-端”连接,屏蔽网络层及以下各层实现技术的差异性,弥补网络层所能够提供服务的不足,实现分布式进程通信。

(4) 在传输层中,传输层协议的硬件或软件称为传输实体。传输实体可能在操作系统内核中,或在一个单独的用户进程中。

(5) 传输层在有效载荷 TPDU 之前加上 TPDU 头,形成了 TPDU 传输协议数据单元。TPDU 头用于传达传输层协议的命令和响应。

(6) TPDU 传送到网络层后,加上 IP 分组头后形成 IP 分组;IP 分组传送到数据链路层后,加上帧头、帧尾形成帧。

从以上分析中可以看出,从网络体系结构的角度来看,传输网络只包括物理层、数据链路层与网络层。传输网络是由电信公司提供服务。如果传输网络提供的服务不可靠,那么用户是没有办法去改善传输网络固有的性能参数,只能够通过增加传输层来改善传输网络对最终用户所能提供的服务质量。因此,C 的描述是错误的。

答案:C。

6-1-2 分析:设计该例题的目的是加深读者对应用进程、传输层接口与套接字的理解。在讨论应用进程、传输层接口与套接字时,需要注意以下几个主要问题:

(1) 应用进程是由应用程序开发者开发的,应用程序与传输层的 TCP 或 UDP 协议都是在主机操作系统控制下工作。应用程序的开发者只能够根据需要,在传输层选择 TCP 协议或 UDP 协议,设定相应的最大缓存、最大报文长度等参数。一旦传输层协议类型和参数设定后,传输层协议就在本地主机的操作系统控制下,为应用程序提供确定的服务。

(2) 网络环境中进程通信要解决的第一个问题是进程标识。在一台计算机中,不同的进程可以用进程号或进程标识(process ID)唯一地标识出来。进程号也叫作端口号(port number)。在网络环境中,标识一个进程必须同时使用 IP 地址与端口号。一个 IP 地址与一个进程标识称为一个“套接字(socket)”或“套接字地址(socket address)”。

(3) 服务器套接字地址唯一地定义了服务器应用程序;客户机套接字地址唯一地定义了客户机应用程序。套接字是应用层与传输层之间的接口。由于套接字是建立网络应用程序的可编程接口,因此套接字也叫作应用程序编程接口(API)。

从以上分析中可以看出,A 所描述的“应用进程是在应用程序开发者控制下”提法不正确,应用程序与传输层的 TCP 或 UDP 协议都在主机操作系统的控制下。

答案:A。

6-1-3 分析:设计该例题的目的是加深读者对网络环境中应用进程标识的理解。在讨论网络环境中的应用进程标识时,需要注意以下几个主要问题:

(1) IANA 定义的端口号有 3 类:熟知端口号、注册端口号和临时端口号。

(2) 端口号的数值是取 0~65 535 的整数。

(3) 客户程序使用临时端口号,它是由运行在客户主机上的 TCP/UDP 软件随机选取的。临时端口号数值范围为 49 152～65 535。

(4) TCP/UDP 给每种服务器程序分配了确定的全局端口号,叫作熟知端口号或公认端口号。每个客户进程都知道相应的服务器进程的熟知端口号。熟知端口号值的范围为 0～1023,它是统一分配和控制。

(5) 注册端口号值的范围为 1024～49 151,用户根据需要在 IANA 注册,以防止重复。

(6) TCP/IP 之外的其他传输层协议可能使用与 IANA 不一样的熟知端口号和临时端口号。

需要注意的是,在讨论网络环境中的应用进程标识问题时,人们自然会将关注点放在 TCP/IP 协议上,不太注意不同的操作系统如果采用了不同的传输层协议,那么它们是否都按照 IANA 规定采用相同的熟知端口号和临时端口号,在实际工作中会遇到这类的问题。事实上,有些操作系统不采用 TCP/IP 协议,例如 Xerox 公司的网络系统(XNS)的传输层采用顺序分组协议(SPP)和网间数据报协议(IDP),其中 SPP 协议相当于 TCP 协议,IDP 协议相当于 UDP 协议,那么就有可能使用与 IANA 不一样的熟知端口号和临时端口号。因此,D 的描述是错误的。

答案:D。

6-1-4 分析:设计该例题的目的是加深读者对 TCP 熟知端口号的理解和记忆。在讨论 TCP 熟知端口号时,需要注意以下几个主要问题:

(1) 互联网标准协议所规定的熟知端口号列表可以在 http://www.iana.org 中查询。

(2) 表 6-1 给出了 TCP 常用的熟知端口号。

表 6-1 TCP 常用的熟知端口号

端 口 号	服务进程	说 明
20	FTP	数据文件传输协议(数据连接)
21	FTP	控制文件传输协议(控制连接)
23	TELNET	网络虚拟终端协议
25	SMTP	简单邮件传输协议
80	HTTP	超文本传输协议
119	NNTP	网络新闻传输协议
179	BGP	边界路由协议

对照表 6-1 可以看出,D 的描述是错误的。

答案:D。

6-1-5 分析:设计该例题的目的是加深读者对 UDP 熟知端口号的理解。在讨论 UDP 熟知端口号时,需要注意以下几个主要问题:

(1) UDP 服务与端口号的映射表定期在 RFC768 等文本中公布,并可以在大多数 UNIX 主机的/etc/services 文件中得到。

(2) 表6-2给出了UDP常用的熟知端口号。

表6-2 UDP的熟知端口号

端口号	服务进程	说明
7	Echo	将收到的数据报回送到发送器
9	Discard	丢弃任何收到的数据报
11	Users	活跃的用户
13	Daytime	返回日期和时间
17	Quote	返回日期的引用
19	Chargen	返回字符串
53	NameServer	域名服务
67	Bootps	下载引导程序信息的Server端口
68	Bootpc	下载引导程序信息的Client端口
69	TFTP	简单文件传送协议
111	RPC	远程过程调用
123	NTP	网络时间协议
161	SNMP	简单网络管理协议
162	SNMP	简单网络管理协议

对照表6-2可以看出,B的描述是错误的。

答案:B。

6-1-6 分析:设计这道习题的目的是加深读者对传输层进程连接表示方法的认识。

(1) IANA定义的端口号有熟知端口号、注册端口号和临时端口号。

(2) 服务器程序分配的熟知端口号值的范围为0~1023。

(3) 客户程序使用的临时端口号数值范围为49 152~65 535。

(4) 服务器端的端口号53是用于标识DNS服务器进程的。

因此,题目给出的客户端标识与服务器TCP连接的五元组中有两点错误:

(1) 服务器端的端口号53是用于标识DNS服务器进程,DNS协议的传输层使用的是UDP协议,不是TCP协议。

(2) 对应客户程序应该使用临时端口号,数值范围为49 152~65 535,而这个五元组中客户程序使用的是1002,属于熟知端口号范围0~1023的值。

答案:

这个五元组的标识是错误的。

错误出在两处:

(1) 服务器端的端口号53是用于标识DNS服务器进程,DNS协议的传输层使用的是UDP协议,不是TCP协议。

(2) 客户程序使用的是服务器熟知端口号范围的值。

6.2 UDP 协议

6-2-1 分析：设计该例题的目的是加深读者对 UDP 协议的主要特点的理解。在讨论 UDP 协议时，需要注意以下几个主要问题：

(1) UDP 是一种无连接的、不可靠的传输层协议。

(2) UDP 是一种面向报文的传输层协议。

(3) UDP 报文长度是固定的 8 字节。报头主要有端口号、长度、检验和等字段。

(4) UDP 校验和用来检验整个用户数据报在传输中是否出现差错。

(5) UDP 检验和包括伪报头、UDP 报头及应用层数据。UDP 检验和字段是可选项。

从以上的讨论中可以看出，A 的描述是错误的。

答案：A。

6-2-2 分析：设计该例题的目的是加深读者对 UDP 协议报文传输特点的理解。

讨论 UDP 面向报文的传输特点，需要注意以下几个基本问题：

(1) UDP 对于应用程序提交的报文，在添加了 UDP 协议头部，构成一个 TPDU 之后就向下提交给 IP 层。

(2) UDP 对应用程序提交的报文既不合并，也不拆分，而是保留原报文的长度与格式。接收方会将发送方提交传送的报文原封不动地提交给接收方应用程序。因此，在使用 UDP 协议时，应用程序必须选择合适长度的报文。

(3) 如果应用程序提交的报文太短，则协议开销相对较大；如果应用程序提交的报文太长，则 UDP 向 IP 层提交的 TPDU 可能在 IP 层被分片，这样也会降低协议的效率。

因此，D 的描述是错误的。

答案：D。

6-2-3 分析：设计该例题的目的是检查读者对 UDP 协议报头结构以及 UDP 协议熟知端口号的理解。

(1) UDP 协议报头结构。

UDP 用户数据报的格式如图 6-1 所示。UDP 用户数据报有固定 8B 的报头。

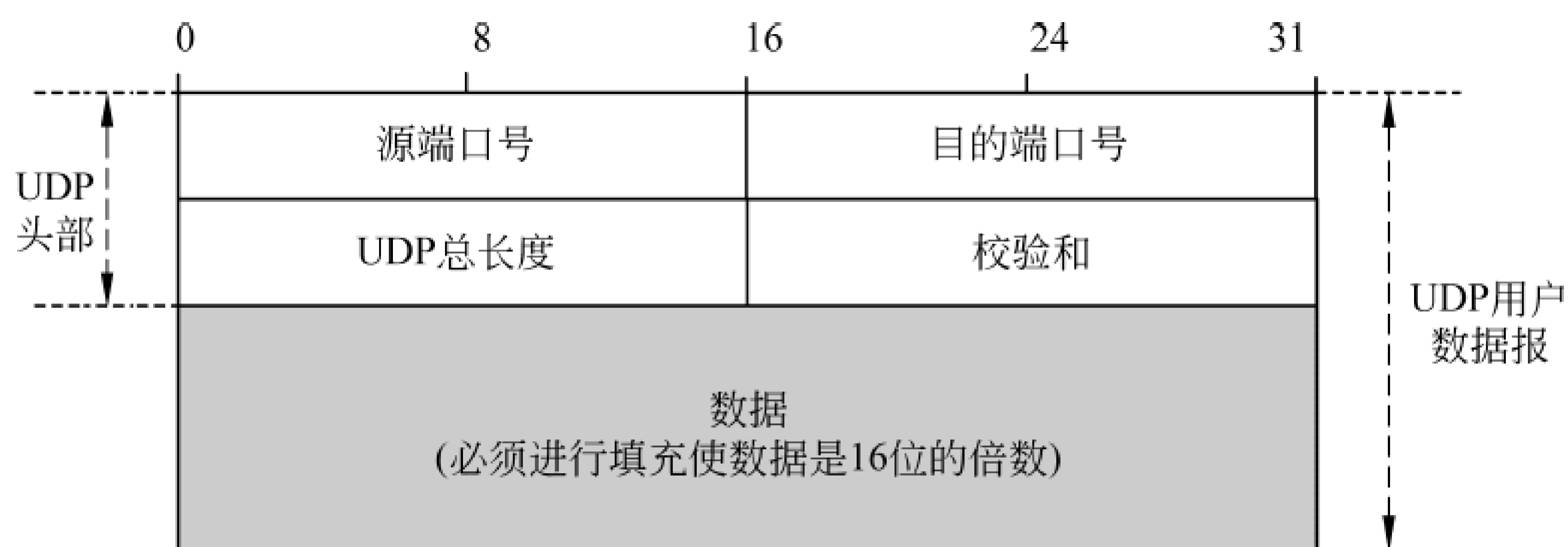


图 6-1 UDP 用户数据报的格式

(2) UDP 协议熟知端口号。

UDP 的熟知端口号如表 6-2 所示。

计算：

根据 UDP 报头的结构，已知的十六进制数为 06 32 00 45 00 1C E2 17，可以分为源端口

号、目的端口号、UDP总长度、校验和4个部分。

(1) 源端口号为十六进制数06 32,转换成十进制数为1586。

(2) 目的端口号为十六进制数00 45,转换成十进制数为69。根据表6-2判断,使用该UDP的服务器类型为简单文件传送协议(TFTP)。

(3) UDP总长度为十六进制数00 1C,转换成十进制数为28。UDP固定报头长度为8字节,用户数据长度为28－8＝20(B)。

(4) 校验和为十六进制数E2 17,转换成二进制数为1110 0010 0001 0111。

答案:

(1) 源端口号为1586;目的端口号为69。

(2) 用户数据长度为20B。

(3) 这个数据报是客户端发出的。

(4) 使用UDP协议的服务器类型是简单文件传送协议(TFTP)。

6-2-4 分析:设计该例题的目的是加深读者对UDP协议适用范围的理解。在讨论UDP协议适用范围时,需要注意确定一种应用程序在传输层是否采用UDP协议有几个考虑的原则:

(1) 系统对性能的要求高于对数据完整性的要求。

这类系统的典型是多媒体应用,因为视频播放程序对数据实时交付的要求高于对数据交付可靠性的要求。为了在互联网上播放视频,用户最关注的是视频流能够尽快和不间断地播放,而对其中个别数据包的丢失并不介意,因为丢失个别数据包并不会对视频节目的播放效果产生重要的影响。如果采用对数据传输可靠性要求很高的TCP协议,那么它有可能因为重传个别丢失的数据包而增大传输延迟,那么反而会产生不利的影响。

(2) 简短的交互式应用。

有一类应用只需要进行简单的请求与应答报文的交互,客户端发出一个简短的请求报文,服务器端回复一个简短的应答报文,在这种情况下应用程序选择UDP协议则更为合适。在这样的系统中,可在应用程序中设置"定时器/重传机制",用来处理由于IP数据分组丢失问题,而不需要选择有确认/重传的TCP协议。在应用程序中增加适当的补充方法有利于提高系统的工作效率。

(3) 多播和广播应用。

UDP支持一对一、一对多与多对多的交互式通信,这点是TCP协议所不支持的。UDP协议头部长度只有8B,比TCP协议头部长度20B短。同时,UDP没有拥塞控制,在网络出现拥塞时不会要求源主机降低报文发送速率,而只会丢弃个别的报文。这对于IP电话、实时视频会议应用来说是适用的。这类应用要求源主机以恒定速率发送报文,在拥塞发生时允许丢弃部分报文。

(4) 需要在软件设计中进一步解决的问题。

简洁、快速、高效是UDP协议的优点,但是由于它不能提供必需的差错控制机制,同时当拥塞严重时缺乏必要的控制与调节机制,因此这些问题需要使用UDP协议的应用程序设计者在应用层设置必要的机制加以解决。UDP是一种适用于实时语音与视频传输的传输层协议。

因此,B的描述是错误的。

答案：B。

6-2-5 分析：设计该例题的目的是加深读者对 UDP 校验和特点的理解。在讨论 UDP 校验和时，需要注意以下几个主要问题：

（1）UDP 检验和字段用来检验整个用户数据报在传输中是否出现差错。

（2）计算检验和时需要在 UDP 数据报之前要增加 12B 的伪头部。

（3）UDP 检验和的检验范围包括伪头部、UDP 报头与从应用层来的数据。

（4）伪头部包括源 IP 地址、目的 IP 地址、UDP 长度等内容。伪头部是因为它本身并不是在 UDP 用户数据报的真正头部，只是在计算时临时与 UDP 用户数据报连接在一起。伪头部只在计算时起作用，它既不向低层传输，也不向高层传送。

（5）UDP 长度指 UDP 数据报的长度，不包括伪头部的长度。

从以上分析中可以看出，D 的描述是错误的。

答案：D。

6.3 TCP 协议

6-3-1 分析：设计该例题的目的是加深读者对 TCP 协议主要特点的理解。在讨论 TCP 协议的主要特点时，需要注意以下几个主要问题：

（1）支持面向连接的传输服务。

面向连接对提高系统数据传输的可靠性是十分重要的。应用程序在使用 TCP 传送数据之前，必须在源进程端口与目的进程端口之间建立一条传输连接。每个 TCP 连接唯一地被通信双方端口号所标识。每个 TCP 连接是为通信双方的一次进程通信提供服务。

（2）支持字节流的传输。

由于 TCP 协议同样建立在不可靠的网络层 IP 协议之上，IP 不能提供任何可靠性机制，因此 TCP 的可靠性完全由自己实现。TCP 协议支持字节流传输的过程是一个无数据丢失、重复和乱序的数据传输过程。由于 TCP 在传输过程中将应用程序提交的数据看成是连串的、无结构的字节流，因此在接收端应用程序数据字节的起始与终结位置必须由应用程序自己去确定。

（3）支持全双工服务。

TCP 允许通信双方的应用程序在任何时候都可以发送数据。由于通信的双方都设置有发送和接收缓冲区，应用程序将要发送的数据字节提交给发送缓冲区，数据字节的实际发送过程由 TCP 协议来控制；而接收方在接收到数据字节之后也将它存放到接收缓冲区，高层应用程序在它合适的时间到缓冲区中读取数据。

（4）支持同时建立多个并发的 TCP 连接。

根据应用程序的需要，TCP 协议支持一个服务器与多个客户端同时建立多个 TCP 连接，同时也支持一个客户端与多个服务器同时建立多个 TCP 连接。TCP 软件将分别管理多个 TCP 连接。TCP 协议理论上可以支持同时建立上百，甚至上千条这样的连接，但是建立并发连接的数量越多，每条连接共享的资源就会越少。

（5）支持可靠服务。

TCP 是一种可靠的传输服务协议，它使用确认机制来检查数据是否安全和完整地到达，并且提供拥塞控制功能。TCP 支持可靠数据通信的关键是它对发送和接收的数据进行

跟踪、确认与重传,以保证数据能够到达接收端。需要注意一个问题,TCP 协议是建立在不可靠的网络层 IP 协议之上,一旦 IP 及以下层出现传输错误,TCP 协议只能够不断地进行重传,试图弥补这次传输出现的问题。因此,传输层传输的可靠性是建立在网络层的基础上,同时也就会受到它的限制。

从以上讨论中可以看出,TCP 支持字节流传输,但不能够确定接收端应用程序数据字节的起始与终结位置。因此,D 的描述是不正确的。

答案:D。

6-3-2 分析:设计该例题的目的是加深读者对 TCP 与 UDP 协议特点的理解。在讨论 TCP 与 UDP 协议特点时,可以参考 TCP 与 UDP 协议的比较(见表 6-3)。

表 6-3 TCP 与 UDP 协议的比较

特征/描述	TCP	UDP
一般描述	允许应用程序可靠地发送数据,功能齐全	简单、高速,只负责将应用层与网络层衔接起来
面向连接或无连接	面向连接,在 TPDU 传输之前需要建立 TCP 连接	无连接,在 TPDU 传输之前不需要建立 UDP 连接
与应用层的数据接口	基于字节流,应用层不需要规定特定的数据格式	基于报文,应用层需要将数据分成包来传送
可靠性与确认	可靠报文传输,对所有的数据均要确认	不可靠,不需要对传输的数据确认,尽力而为地交付
重传	自动重传丢失的数据	不负责检查是否丢失数据和重传
开销	低,但高于 UDP	很低
传输速率	高,但低于 UDP	很高
适用的数据量	从少量到几个 GB 的数据	从少量到几百个字节的数据
适用的应用类型	对传送的数据可靠性要求较高的应用,如文件与报文传输	发送数量比较少,以及对数据传输可靠性要求较低的应用,如 IP 电话、实时视频会议、多播与广播

在比较之后会发现,D 对 TCP 传输速率高于 UDP 的描述是错误的。

答案:D。

6-3-3 分析:设计该例题的目的是加深读者对 TCP 报头格式的理解。在讨论 TCP 报头格式时,需要注意以下几个主要问题:

(1) 报头长度为 20～60B,其中固定部分为 20B,选项部分最多为 40B。

(2) 报头包括的字段有端口号、序号、确认号、报头长度、控制、窗口、紧急指针、选项与检验和。

(3) 端口号字段:源端口号与目的端口号。每个端口号字段长度为 2B,分别表示发送该报文段的应用进程的源端口号与接收进程的目的端口号。

(4) 序号字段:发送字节流中的每字节的顺序号,长度为 32bit,数值范围在 0～4 284 967 295。

(5) 确认号字段:表示出一个进程已经正确地接收了序号为 N 的字节,要求发送方下一个应该发送序号为 $N+1$ 的字节的报文段,长度为 32bit。

(6) 报头长度字段：以4B为单元来计算的报头长度，数值范围在5～15。

(7) 控制字段：定义了6种用于TCP的连接建立和终止、流量控制，以及数据传送的控制位或标志位。

(8) 窗口字段：长度为16bit，表示要求对方必须维持的以字节为单位大小的窗口。

(9) 紧急指针字段：长度为16bit，只有紧急标志URG=1时，该字段有效，表示报文段中包括紧急数据。

(10) 选项：TCP报头可以有多达40B的选项字段。选项包括以下两类：单字节选项和多字节选项。单字节选项有两个：选项结束和无操作。多字节选项有三个：最大报文段长度、窗口扩大因子与时间戳。

(11) 校验和：计算校验和与UDP校验和的过程一样。但是，UDP中的校验和是可选的，而对TCP来说是必须有的。与UDP校验和一样，需要有伪头部，唯一不同的是IP分组头中协议字段的值是6。

从以上分析中可以看出，控制字段定义了6种用于TCP连接、流量控制，及数据传送的控制位或标志位。因此，C的描述是错误的。

答案：C。

6-3-4 分析：设计该例题的目的是加深读者对TCP最大段长度的理解。在讨论TCP最大段长度时，需要注意以下几个主要问题：

(1) TCP协议对报文数据部分最大长度有一个规定，这个值称为最大段长度MSS。

(2) MSS是TCP报文中数据部分的最大字节数限定值，不包括报头长度。

(3) 选择MSS值时需要考虑的因素主要是：协议开销、IP分片长度、发送和接收缓冲区的限制等。

(4) MSS的默认值是536B。

(5) 如果对于某些应用，MSS默认值不适合，编程人员可以在建立TCP连接时，使用SYN报文中最大段长度选项来协商。TCP允许连接双方可以选择使用不同的MSS值。

(6) TCP报文段的最大长度与窗口长度概念是不同的。窗口长度是TCP协议为保证字节流传输的可靠性，接收端通知发送方下一次可以连续传输的字节数。最大段长度MSS是在构成一个TCP报文段时，最多可以在报文的数据字段中放置的数据字节数量。MSS值的确定与每次传输字节流的窗口大小无关。

从以上分析中可以看出，TCP报文段的最大长度MSS与窗口长度是完全不同的两个概念，其数值没有对应关系。因此，C的描述是错误的。

答案：C。

6-3-5 分析：设计这道练习题的目的是帮助读者理解TCP报文段确认机制。

主机A第一个报文段的序号是201，长度为100B，第一个报文段的序号为201～300；第二个报文段长度为200B，第二个报文段的序号为301～500；第二个报文段长度为300B，第二个报文段的序号为501～800。

那么，在主机B正确接收这3个报文段之后，通过确认序号通知主机A：下一个报文段序号为801。

主机B通知主机A用"下一个报文段开始的序号为801"来表示：已正确接收序号201～800的报文段，下一个报文段第一个字节的序号为801。

答案：主机B发送的确认序号为801。

6-3-6 分析：设计本例题的目的是检查读者对于TCP协议字节流传输特点，以及报文段序号编号规则的理解。

(1) 由于TCP协议是面向数据流的，因此需要给发送的每个字节编号。

(2) TCP协议的数据传输单元叫做报文段(segment)。

(3) 报文段序号字段长度为32位。本报文段数据的第1字节的顺序号作为报文段的序号。

计算：

(1) 第1个报文段序号范围：10010～11009；

(2) 第2个报文段序号范围：11010～12009；

(3) 第3个报文段序号范围：12010～13009；

(4) 第4个报文段序号范围：13010～14009；

(5) 第5个报文段序号范围：14010～14209。

答案：5个报文段的序号范围分别为10010～11009、11010～12009、12010～13009、13010～14009与14010～14209。

6-3-7 分析：设计这道习题的目的是帮助读者加深对RTT变量值估算方法的理解。

(1) TCP使用了4种计时器：重传计时器、坚持计时器、保持计时器和时间等待计时器。其中，重传计时器用来控制丢失或丢弃的报文段。从发送数据到收到确认所需的往返时间(RTT)呈动态变化。

(2) TCP采用一种适应性重传算法。TCP监视每条连接的性能，由此推算出合适的时间片，当连接性能发生变化时，TCP随即改变时间片值。

(3) TCP计算时间片的公式如下：$\text{Timeout}=\beta\times\text{RTT}$

其中，β为一个大于1的常数加权因子，RTT为估算的往返时间。

(4) RTT是一个加权平均值，其计算公式如下：

$$\text{RTT}=\alpha\times\text{Old_RTT}+(1-\alpha)\times\text{New_Round_Trip_Sample}$$

其中，Old_RTT是上一个往返时间估算值，New_Round_Trip_Sample是实际测出的前一个段的往返时间(样本)。α也是一个常数加权因子($0\leqslant\alpha<1$)。

计算：从题意中可以找出以下的已知条件。

$\alpha=0.9$，Old_RTT$=35$ms，$M1=26$ms，$M2=32$ms，$M3=24$ms。

根据公式可以计算出：

$$\text{RTT1}=0.9\times35+(1-0.9)\times26\approx34.1(\text{ms})$$

$$\text{RTT2}=0.9\times34.1+(1-0.9)\times32\approx33.9(\text{ms})$$

$$\text{RTT3}=0.9\times33.9+(1-0.9)\times24\approx32.9(\text{ms})$$

答案：

新的估计往返延时值为RTT1=34.1(ms)、RTT2=33.9(ms)、RTT3=32.9(ms)。

6-3-8 分析：设计该例题的目的是加深读者对控制TCP可靠传输方法的理解。在讨论TCP可靠传输时，需要注意以下几个主要问题：

(1) TCP是面向连接的协议，在传输TCP用户数据报之前，必须首先建立传输连接；在用户数据流传输过程中，需要维护传输连接；在用户数据报传输结束时，需要释放传输连接。

(2) 在 TCP 传输连接建立过程中，需要解决三个基本问题：

① 确定通信的双方是否存在。

② 允许双方协商通信参数，例如最大报文段长度、最大窗口长度以及服务质量等。

③ 分配传输实体可以使用的资源，例如缓冲区大小。

(3) TCP 协议的客户进程与服务器进程连接建立需要经过“三次握手”的过程。采用“三次握手”的目的是为防止传输连接过程中出现错误。

(4) TCP 的差错检测是通过校验和、确认和超时来检测出错、丢失、乱序和重复的报文等方法来实现。

从以上分析中可以看出，C 的描述是错误的。

答案：C。

6-3-9 分析：设计这道习题的目的是加深读者对 TCP 报头中“序号”字段意义的理解。

(1) TCP 是面向字节流的，它要为发送字节流中的每个字节都按顺序编号。

(2) 序号字段长度为 32bit，序号范围在 $0\sim(2^{32}-1)$，即 0～4 284 967 295。

(3) 在 TCP 连接建立时，每方需要使用随机数产生器产生一个初始序号 ISN。

(4) 由于是连接双方各自随机产生初始序号，因此一个 TCP 连接的通信双方序号是不同的。

因此，D 的描述是错误的。

答案：D。

6-3-10 分析：设计这道习题的目的是加深读者对 TCP 最大段长度 MSS 概念的理解。

(1) TCP 报文段的最大长度 MSS 是在构成一个 TCP 报文段时，最多可以在报文的数据字段中放置的数据字节数。

(2) 默认的 MSS 值为 536B。如果考虑规定的报头长度为 20B，那么默认的报文段长度就为 556B。

(3) 当然对于某些应用，MSS 默认值也许不一定适用。编程人员希望选择其他的 MSS 值，这个要求可以在建立 TCP 连接时，使用 SYN 报文中最大段长度选项来协商。TCP 允许连接的双方可以选择使用不同的 MSS 值。

因此，B 的描述是错误的。

答案：B。

6-3-11 分析：设计该例题的目的是加深读者对 TCP 窗口、报文段平均往返延时与吞吐量关系的理解。

(1) 发送窗口的大小受接收端接收能力的影响。如果说 TCP 使用的最大窗口为 64KB，也就是说，发送端可以在没有接收到确认的情况下，连续发送 64KB 的数据字节。

(2) 报文段平均往返延时为 20ms，说明在发送 20ms 之后应该能够获得确认信息。因此，可以根据这两个数据计算出最大的吞吐量。条件是发送带宽不存在限制。

计算：

(1) $64\text{KB}=64\times1024\times8=524\ 288(\text{bit})$

(2) $524\ 288\ /(20\times10-3)=26.214\text{M}(\text{bps})$

答案：最大的吞吐量是 26.21 Mbps。

6-3-12 分析：这是一个从 TCP 发送窗口、往返延时、信道带宽反推出一个 TCP 连接

可以达到最大吞吐率、信道利用率的综合性题目。问题表面看比较简单,但是可以检查读者对 TCP 协议工作原理理解的深度。

(1) 往返延时=2×端-端延时

(2) 最大吞吐率=发送窗口值×往返延时

(3) 信道利用率=最大吞吐率/信道带宽

计算:

(1) 往返延时=2×10=20(ms)

(2) 最大吞吐率=(65 535×8)/(20×10-3)=26.214M(bps)

(3) 信道利用率=26.214/1000≈2.62%

答案:最大吞吐率 为 26.214Mbps,信道利用率约为 2.62%。

* **6-3-13** 分析:

这是一道考查读者对 TCP 报文段 MSS、生存时间 TTL 与序号关系连接的综合性习题。完成这道题的难点在于将生存时间 TTL 与序号关系建立起联系。

(1) 生存时间 TTL=30s,表示在 30s 内不允许有相同序号的报文段出现。序号用 8bit 表示最快在 30s 中传输 255 个报文段,每秒钟最多传输 255/30 个报文段。

(2) 每个报文段长度为 128B。

(3) 根据以上两个数据就可以求出每条 TCP 连接能够达到的最高速率。

计算:

(1) 每秒钟最多传输报文段为 255/30=8.5(个)。

(2) 每个报文段长度为 128×8=1024(bit)。

(3) 每条 TCP 连接能达到的最高速率为 1024×8.5=8.704k(bps)

答案:每条 TCP 连接能达到的最高速率为 8.704kbps。

* **6-3-14** 分析:

这是一道考查读者对 TCP 报文段生存时间 TTL 与序号关系连接的综合性练习题。完成这道题的难点在于将生存时间 TTL 与序号关系建立起联系。

(1) 已知序号用 64bit 表示,知道 TCP 报文段的序号最大为 $2^{64}-1=2\times10^{19}-1\approx2\times10^{19}$。注意:由于 TCP 协议是面向字节的,因此,TCP 报文段的最大序号表示最多传输 2×10^{19}B。

(2) 已知传输速率为 75Tbps,如果用字节表示 75Tbps=$(75/8)\times10^{12}$(B/s)≈9.375×10^{12}(B/s)。注意:从另一个角度,它表示按照这样的速率,每秒钟需要消耗 9.375×10^{12}B 的序号。

(3) 已知有多少字节的序号,在光链路上每秒钟消耗的字节数也知道,那么就知道这些序号多少时间消耗完,也就等于知道这段时间内序号不会重复。

计算:

(1) 已知序号位长度为 64bit,那么序号表示最多能够表示 2×10^{19}B。

(2) 已知传输速率为 75Tbps,如果用字节表示 75Tbps=$(75/8)\times10^{12}\approx9.375\times10^{12}$(B/s)。

(3) $(2\times10^{19})/(9.375\times10^{12})=2.13\times10^{6}$(s)。

答案:TCP 报文段的序号用 64bit 表示,在速率为 75Tbps 时,报文段在 2.13×10^{6}s 时

间内不会发生序号重复的现象。

*6-3-15 分析：

这是一道考察读者对 TCP 报文段的端-端延时、吞吐率、传输速率与发送窗口关系连接的综合性练习题。完成这道题的难点在于为端-端延时、吞吐率、传输速率与发送窗口建立起联系。

(1) 已知端-端延时，它的 2 倍就是报文段在发送端与接收端之间的往返延时。

(2) 已知发送速率，只要知道发送窗口长度，就可以得出发送延时。

(3) 已知往返延时与发送延时，用发送窗口长度去除往返延时与发送延时之和，就可以得出实际的传输速率，也就是吞吐量。

计算：设发送窗口长度为 X(B)。

$$往返延时=2\times(128\times10^{-3})=256(ms)$$

依据题意列出方程：

$$8X/(8X/(256\times10^{3})+256\times10^{-3})=120\times10^{3}$$

得

$$X=7228(B)$$

答案：发送窗口长度为 7228B。

6-3-16 分析：基于慢开始、拥塞避免的 AIMD 算法 TCP 拥塞控制过程为：

(1) 当 TCP 连接初始化时，将拥塞窗口 cwnd 设置为 1(单位为 MSS)。设置慢开始时的初始阈值 ssthresh1。在慢开始阶段，当 cwnd 经过几个往返传输之后，按照指数算法已经增长到 SST1 时，进入“拥塞避免”控制阶段。

(2) 进入拥塞避免阶段之后，cwnd 按照线性的方法增长，假如在 cwnd 值达到某个最大值时，发送端检测出现超时，那么拥塞窗口 cwnd 重新回到 1。

(3) 当出现一次网络拥塞之后的慢开始阈值 ssthresh2 是出现超时的 cwnd 最大值的 1/2，然后重新开始慢开始与拥塞避免的过程。

计算：

(1) 慢开始。

当 TCP 连接初始化时，将 cwnd 设置为 1。慢开始 ssthresh1 的阈值设置为 8。在慢开始阶段，当 cwnd 经过 3 个往返传输之后，按照指数算法已经增长到 8 时，进入“拥塞避免”控制阶段。这个过程经过 3 个往返的过程。

(2) 拥塞避免。

进入拥塞避免阶段之后，cwnd 按照线性的方法增长，cwnd 值从 8 上升到 12，经过 4 个往返过程。

(3) 当 cwnd=12 时，发送端检测到出现超时，那么第 8 个往返时，拥塞窗口 cwnd 重新回到 1。

(4) 重新进入慢开始与拥塞控制。

当出现一次网络拥塞之后的慢开始阈值 ssthresh2 设置是出现超时的 cwnd 最大值的 1/2，即 ssthresh2=12/2=6，重新开始慢开始与拥塞避免的过程。

(5) 第 8 个往返的拥塞窗口 cwnd=1；按照指数增长，第 9 个往返的 cwnd=4；第 10 个往返不能超过 ssthresh2=6，cwnd=6。

(6) 第11个往返的cwnd在6的基础上加1,cwnd=7;以此类推,第12、13、14、15个往返的cwnd分别应该等于8、9、10。

按照上述分析和计算的TCP拥塞控制过程如图6-2所示。

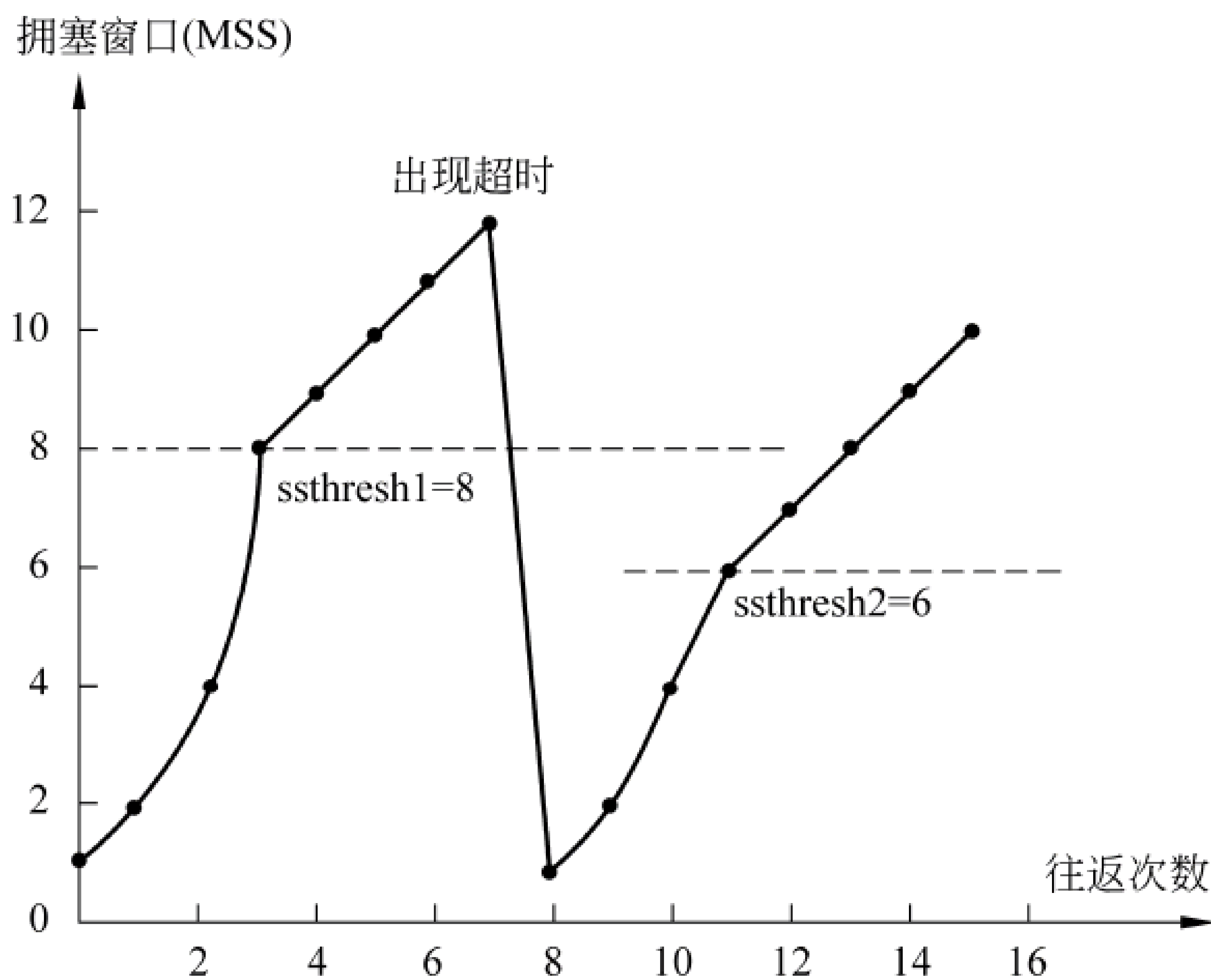


图6-2 TCP拥塞控制示意图

答案:第1个往返到第15个往返的cwnd值分别为2、4、8、9、10、11、12、1、2、4、6、7、8、9与10。

6-3-17 分析:

(1) Ethernet帧的数据字段长度最大为1500B,而TCP用户数据长度为8192B,因此必须分片。

(2) 如果每个分片长度取1500B,而TCP报头长度为20B,因此分片用户数据长度可以是1480B。

计算:

(1) UDP用户数据长度为8192B,分片用户数据长度可以是1480B,那么可以分为6个分片,其中前5个分片长度为1480B,第6个分片长度为792B。

(2) 每个片的数据字段长度与片偏移值

第1片:长度1480B,偏移值0

第2片:长度1480B,偏移值2960

第3片:长度1480B,偏移值4440

第4片:长度1480B,偏移值5920

第5片:长度1480B,偏移值7400

第6片:长度792B,偏移值8192

答案:必须分片;可以分为6个分片,其中前5个分片长度为1480B,第6个分片长度为792B;第1片长度为1480B,偏移值为0,第2片长度为1480B,偏移值为2960,以此类推,第6片长度为792B,偏移值为8192。

6-3-18 分析:TCP使用了4种计时器:重传计时器、坚持计时器、保持计时器和时间等待计时器。了解4种计时器的特点,对于深入理解TCP工作原理很重要。

（1）保持计时器（Keepalive Timer）。

保持计时器的特点主要表现在以下几点：

① 设置保持计时器的目的是为了防止TCP连接处于长时期空闲状态。

② 当服务器端收到客户端的报文时，就将保持计时器复位。如果服务器端过了设定的时间没有收到客户端的信息，它就发送探测报文。

③ 如果发送10个探测报文（每个相隔75s）还没有响应，就假设客户端出现故障，进而终止该连接。

（2）时间等待计时器（TIME-WAIT Timer）。

时间等待计时器的特点主要表现在以下几点：

① 设置时间等待计时器的目的是为了保证TCP连接释放过程正常地进行。

② 当TCP关闭一个连接时，客户端进入"时间等待"状态。

③ 等待2个最长报文寿命（MSL）时间之后，才真正进入"关闭"状态。

（3）重传计时器（Retransmission Timer）。

重传计时器的特点主要表现在以下几点：

① 设置重传计时器的目的是控制报文确认与等待重传的时间。

② 当发送端TCP发送一个报文时，首先将它的一个副本放入重传队列，同时启动一个重传计时器。

③ 重传计时器设定一个值，然后开始倒计时。

④ 在重传计时器倒计时到0之前收到确认，表示该报文传输成功；如果在计时器倒计时到0时没收到确认，表示该报文传输失败，准备重传该报文。

（4）坚持计时器（Persistence Timer）。

① 设置坚持计时器的目的是防止发送端因无休止地等待接收端的通知造成的死锁。

② 当发送端的TCP收到一个零窗口通知时，就启动坚持计时器。

③ 当坚持计时器时间到，发送端的TCP就发送一个零窗口探测报文。零窗口探测报文的作用是提示接收端：非零窗口通知丢失，必须重传。

④ 坚持计时器的值设置为重传时间的数值，最大为60s。如果发出的第一个零窗口探测报文没有收到应答，则需发送第二个零窗口探测报文，直到收到非零窗口为止。

从以上分析中可以看出，D的描述是错误的。

答案：D。

6-3-19 分析：设计这道习题的目的是加深读者对TCP连接建立三次握手过程的理解。

主机A向主机B发送一个建立TCP连接的（SYN＝1，seq＝11180）报文段，主机B接收连接请求，那么应答报文中：

（1）SYN＝1，ACK＝1。

（2）ACK应答中的ack＝11180＋1＝11181，表示对正确接收到seq＝11180报文段的确认。

（3）ACK应答中的seq＝56421值取决于接收端，只要在合理的范围内均可。

因此，D的描述是正确的。

答案：D。

6-3-20 分析：设计这道习题的目的是加深读者对 TCP 连接建立过程的理解。

(1) 主机 A 向主机 B 建立了一个 TCP 连接，主机 A 连续向主机 B 发送了 200B、300B 与 400B 共 3 个报文段。第 3 个报文段的序号是 900。如果主机 B 只正确地接收到第 1 个和第 3 个报文段，那么主机 B 向主机 A 发送的确认序号应该是第 2 个报文段的序号。

(2) 第 3 个报文段的序号是 900，是指第 3 个报文段第一字节的序号是 900。

(3) 第 2 个报文段长度为 300B，那么它的第一字节的序号应该为 900－300＝600。

(4) 主机 B 只正确地接收到第 1 个和第 3 个报文段，那么它希望接收的是第 2 个报文段。

因此，主机 B 向主机 A 发送的确认序号应该是第 2 个报文段的序号 600。

答案：600。

6-3-21 设计这道习题的目的是帮助读者熟悉报文序号的使用。

在 TCP 连接上连续发送 4 个数据长度为 1500B 的报文段。

如果第一个报文段的第一字节序号为 5001，那么报文数据的长度为 1500B，那么第二个报文第一字节的序号就是 6501。第二个报文传输 1500B，那么第三个报文的第一字节的序号就是 8001。第三个报文的序号为 8001～9500。因此，C 的描述是正确的。

答案：C。

* **6-3-22** 分析：设计这道题的目的是帮助读者掌握 TCP 连接建立的“三次握手”与连接释放的“四次握手”的概念与过程。示意图如图 6-3 所示。

Sniffer Portable - Local, Ethernet (Line speed at 100 Mbps) - [a2.cap: Filtered 3, 36/25000 Ethernet Frames, Filter: Matrix]

File Monitor Capture Display Tools Database Window Help

No	Source Addes	Dest. Addes	Summary	Len(B)
3	202.1.64.166	211.80.20.2	DNS: NAME=www.it.com	77
4	211.80.20.2	202.1.64.166	DNS: IP=201.8.2.2 NAME=www.itnk.com	165
5	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 SYN=1 SEQ=10020	62
6	201.8.2.2	202.1.64.166	TCP: S=80 D=1298 SYN=1 ACK=1 SEQ=25609 ack= ①	62
7	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 ACK=1 SEQ= ② ack= ③	60
8	202.1.64.166	201.8.2.2	HTTP: Port=1535 GET/HTTP/1.1	568

(a) TCP连接建立的三次握手过程

Sniffer Portable - Local, Ethernet (Line speed at 100 Mbps) - [a2.cap: Filtered 3, 36/25000 Ethernet Frames, Filter: Matrix]

File Monitor Capture Display Tools Database Window Help

No	Source Addes	Dest. Addes	Summary	Len(B)
	………			
23	202.1.64.166	201.8.2.2	数据 Len=100 S=1298 D=80 SQL=16651 ack=68830	1080
24		202.1.64.166	数据 Len=1005 S=80 D=1298 SQL=68831 ack=16751	165
25	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 FIN=1 SEQ=16955 ack=60036	62
26	201.8.2.2	202.1.64.166	TCP: S=80 D=1298 ACK=1 SEQ= ④ ack= ⑤	62
27	201.8.2.20	202.1.64.166	TCP: S=80 D=1298 FIN=1 ACK=1 SEQ= ⑥ ack=16955	60
28	202.1.64.166	201.8.2.2	TCP: S=1298 D=80 ACK=1 SEQ= ⑦ ack= ⑧	60

(b) TCP连接释放的四次握手过程

图 6-3 TCP 连接建立与连接释放过程示意图

(1) 注意“三次握手”过程示意图中的数据。

①处 ack 的数据是对客户端上一个报文 5 的捎带确认，报文 5 的序号是 SEQ＝10020，因此①处 ack＝10020＋1＝10021。②处是报文 7 的序号，因此②SEQ＝10021；③处是报文 7 的序号，它应该等于报文 6 的序号加 1，即 ack＝25609＋1＝25610。

(2) 注意“四次握手”过程示意图中的数据。

④处是报文26的序号，它应该等于报文25中的ack数值，④SEQ＝60036。⑤处是对报文25的确认，因此ack＝16955＋1＝16956。⑥处是报文27的序号，它是继报文26之后服务器端发往客户端的报文，因此它的序号是在④的序号上加1，即⑥SEQ＝60037。⑦处是对报文28的序号，它应该等于报文27的ack值，因此⑦SEQ＝16956。⑧处是对报文27的确认，因此⑧处确认ack等于⑥处SEQ值加1，即ack＝60037＋1＝60038。

答案：

① 10021　② 10021　③ 25610　④ 60036

⑤ 16956　⑥ 60037　⑦ 16958　⑧ 60038

6-3-23　分析：设计这道习题的目的是帮助读者深入理解TCP协议头的结构。

TCP协议头部结构如图6-4所示。

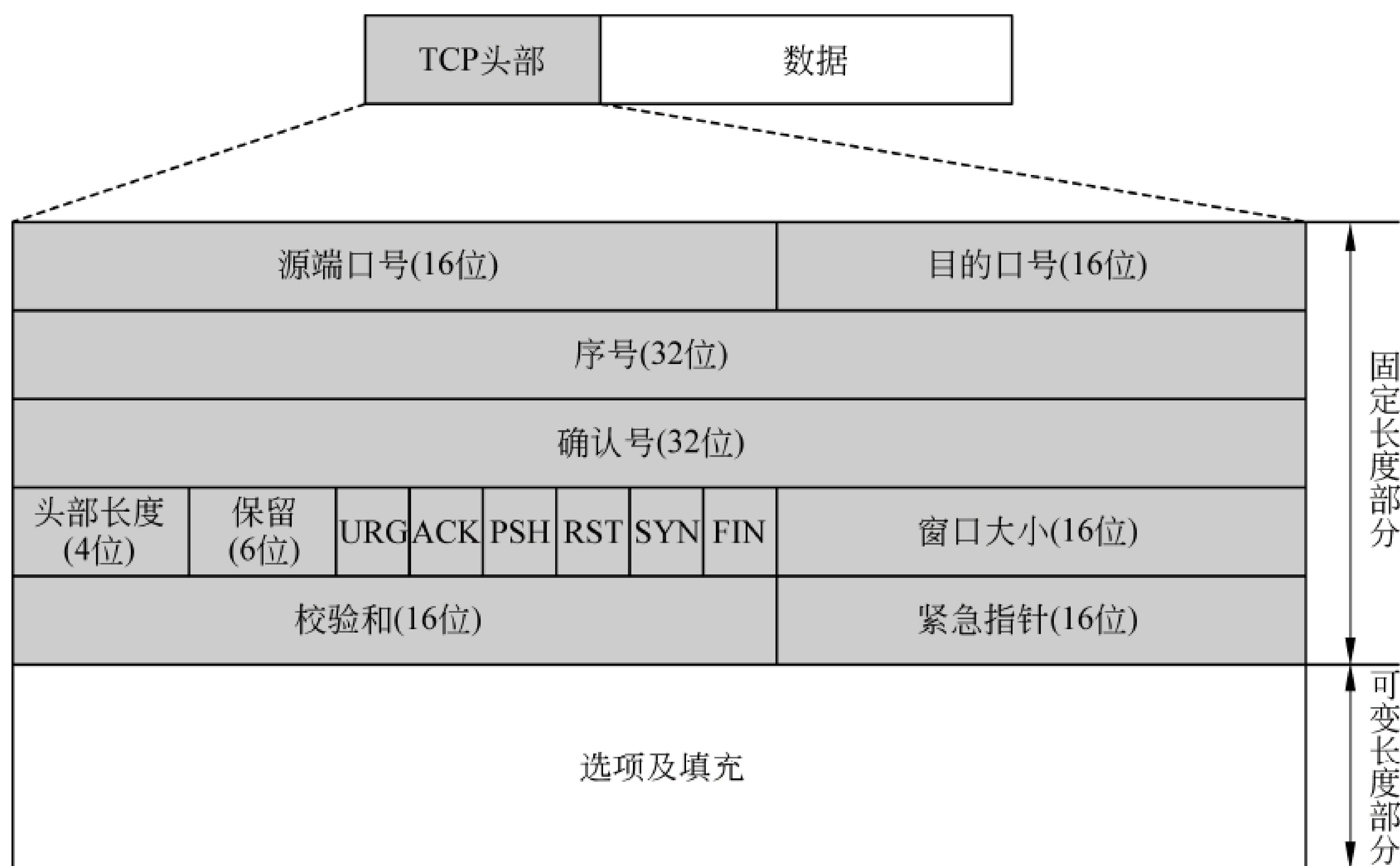


图6-4　TCP头部结构

用十六进制表示的一个TCP报文的头部数据为：

0d 28 00 15 00 00 00 06 00 00 00 00 70 02 40 00 c0 29 00 00。

(1) 源端口号对应第1、2字节，值为：0d 28H，转化成十进制为：3368。

目的端口号对应第3、4字节，值为：00 15H，转化成十进制为：21。

(2) 序列号对应第5～8字节，值为：00 00 00 06H，seq＝6。

确认号对应第9～12字节，值为：00 00 00 00，ack＝0。

(3) TCP头部长度对应第13字节的前4位，值为：7。由于TCP报头长度是以4B为一个单位计算的，因此报头长度为28B。其中，20B为固定报头的长度，8B为选项长度。

(4) 从目的端口号为21可以看出，这是FTP应用产生的TCP连接。

(5) TCP连接的状态可以从第14字节的ACK、SYN与FIN字段值中判断。

第14字节是02，用二进制表示为：0000 0010。

因此，ACK＝0，SYN＝1，FIN＝0。

FIN=0,表示还有数据要传输,目前处于连接建立阶段;

ACK=0、SYN=1,表示客户端与服务器端的第一次握手。

答案:

(1) 源端口号为:3368。

目的端口号为:21。

(2) 序列号 seq=6。

确认号 ack=0。

(3) TCP头部长度为28B。其中,20B为固定报头的长度,8B为选项长度。

(4) 从目的端口号为21可以看出,这是FTP应用产生的TCP连接。

(5) 目前处于建立TCP连接的客户端与服务器端的第一次握手阶段。

6-3-24 分析:设计这道习题的目的是帮助读者将IP协议、TCP协议与应用层协议贯穿起来思考,深入地理解计算机网络的工作原理,灵活地应用网络知识。

已知:

- 主机H通过快速以太网连接到Internet,IP地址为192.168.0.8。
- 服务器S的IP地址为211.68.71.80。
- 主机H与服务器S建立了TCP连接。
- 用软件工具捕获的主机H的5个IP分组的前40B的内容如表6-4所示。

表6-4 5个IP分组的前40B内容

编号	IP分组的前40B的内容(十六进制)
1	45 00 00 30 01 9b 400 00 80 06 1d e8 c0 a8 00 08 d3 44 47 50 0b d9 13 88 84 6b 41 c5 00 00 00 00 70 02 43 80 5d b0 00 00
2	45 00 00 30 00 00 40 00 31 06 6e 83 d3 44 47 50 c0 a8 00 08 13 88 0b d9 e0 59 9f ef 84 6b 41 c6 70 12 16 d0 37 e1 00 00
3	45 00 00 28 01 9c 40 00 80 06 1d ef c0 a8 00 08 d3 44 47 50 0b d9 13 88 84 6b 41 c6 e0 59 9f f0 50 18 43 80 c6 55 00 00
4	45 00 00 38 01 9d 40 00 80 06 1d de c0 a8 00 08 d3 44 47 50 0b d9 13 88 84 6b 41 c6 e0 59 9f f0 50 18 43 80 c6 55 00 00
5	45 00 00 28 68 11 40 00 31 06 06 7a d3 44 47 50 c0 a8 00 08 13 88 0b d9 e0 59 9f f0 84 6b 41 d6 50 10 16 d0 57 d2 00 00

(1) 依据IP分组结构(见图6-5)对数据进行分析。

IP分组头固定部分长度为20B,之后是可选部分。

第一步,分析表6-4中数据的值与含义。

45 00 00 30   01 9b 40 00   80 06 1d e8   c0 a8 00 08   d3 44 47 50

0b d9 13 88   84 6b 41 c5   00 00 00 00   70 02 43 80   5d b0 00 00

① 判断分组头长度。

45H=4×16+5=69,对应的二进制数是0100 0101。其中,0100分组头第一个字段"版本",版本值=4,表示该分组使用的是IPv4协议;0101等于5,表示分组头长度为5,根据IP分组头表示的规定,每4B为1行,5×4B=20B,表示该分组头没有选项部分。表6-5中编号为1的40B数据的后20B为TCP报文段头部。

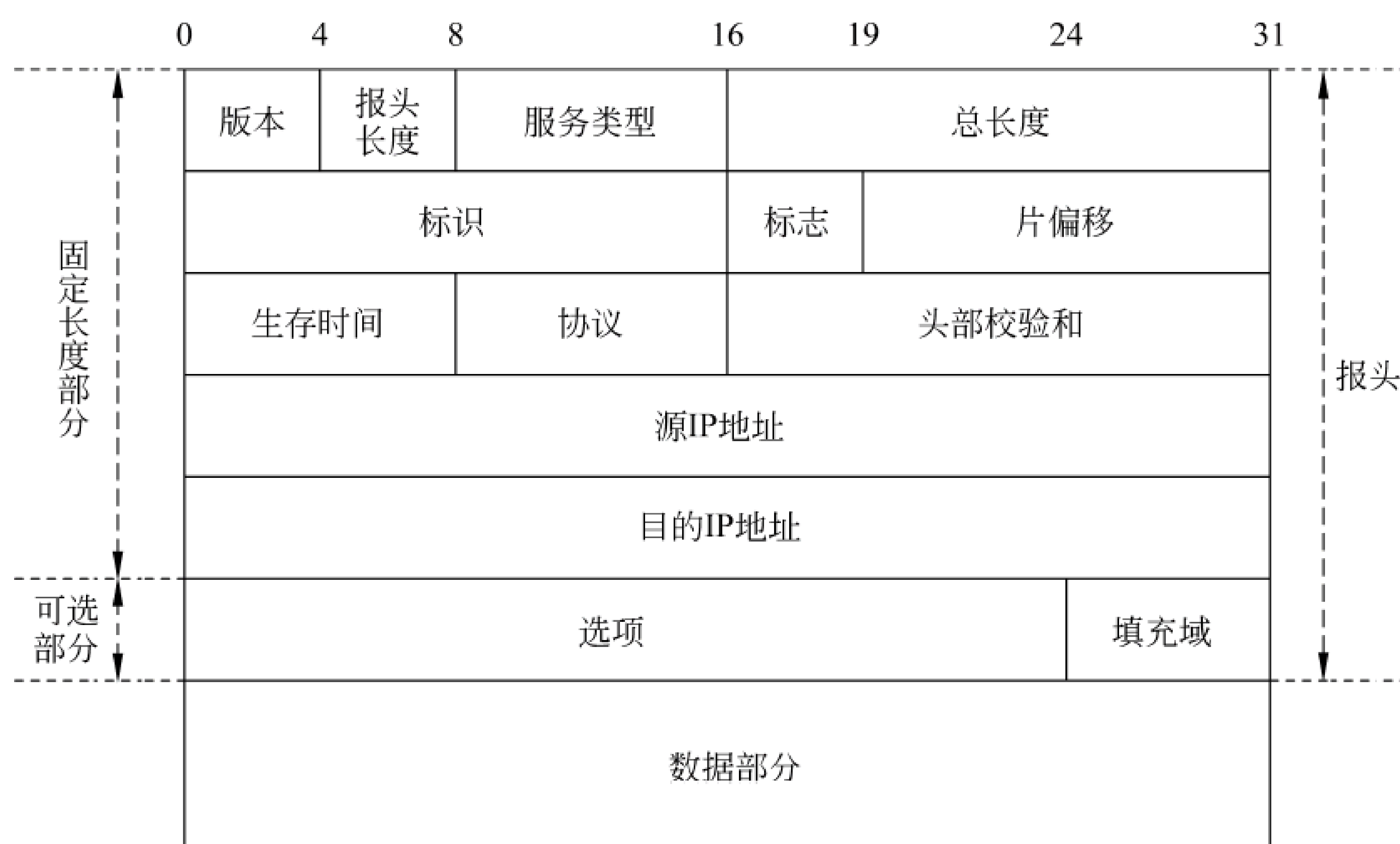


图 6-5　IP 分组结构

② 分析源 IP 地址与目的 IP 地址。

数据中第 13～16 字节为源地址：c0 a8 00 08H，计算 c0H＝16×12＝192，c0H＝16×10＋8＝168，08H＝8，如果用点分十进制表示则为：192.168.0.8，主机 H 的 IP 地址。

同理，数据中第 17～20 字节为源地址：d3 44 47 50H，点分十进制表示为：211.68.71.80，服务器 S 的 IP 地址。

用同样的方法看编号 2～5 数据中第 13～16 字节与第 17～20 字节，可以得出：

- 编号 1 的 IP 分组是由主机 H 发送给服务器 S。
- 编号 2 的 IP 分组是由服务器 S 发送给主机 H。
- 编号 3 的 IP 分组是由主机 H 发送给服务器 S。
- 编号 4 的 IP 分组是由主机 H 发送给服务器 S。
- 编号 5 的 IP 分组是由服务器 S 发送给主机 H。

(2) 依据 TCP 报文结构(见图 6-6)对数据进行分析。

TCP 报头长度为 20～60B，其中固定部分长度为 20B；选项部分长度可变，最多为 40B。分析：

- 编号 1 的数据：

① TCP 头部的 SYN 与 FIN 字段对应第 34 字节的数据。第 34 字节的数据为：02H，用二进制数表示为 10，在 TCP 协议中表示：SYN＝1，ACK＝0。

② TCP 报文段序号对应第 25～28 字节的数据对应“序号”与“确认号”，数据十六进制值分别为：

seq＝84 6b 41 c5

ack＝00 00 00 00

- 编号 2 的数据：

① TCP 头部的 SYN 与 FIN 字段对应第 34 字节的数据。第 34 字节的数据为：12H，用十进制数表示为 18，用二进制表示为 0001 0010，对照在 TCP 报文头格式，为：SYN＝1，

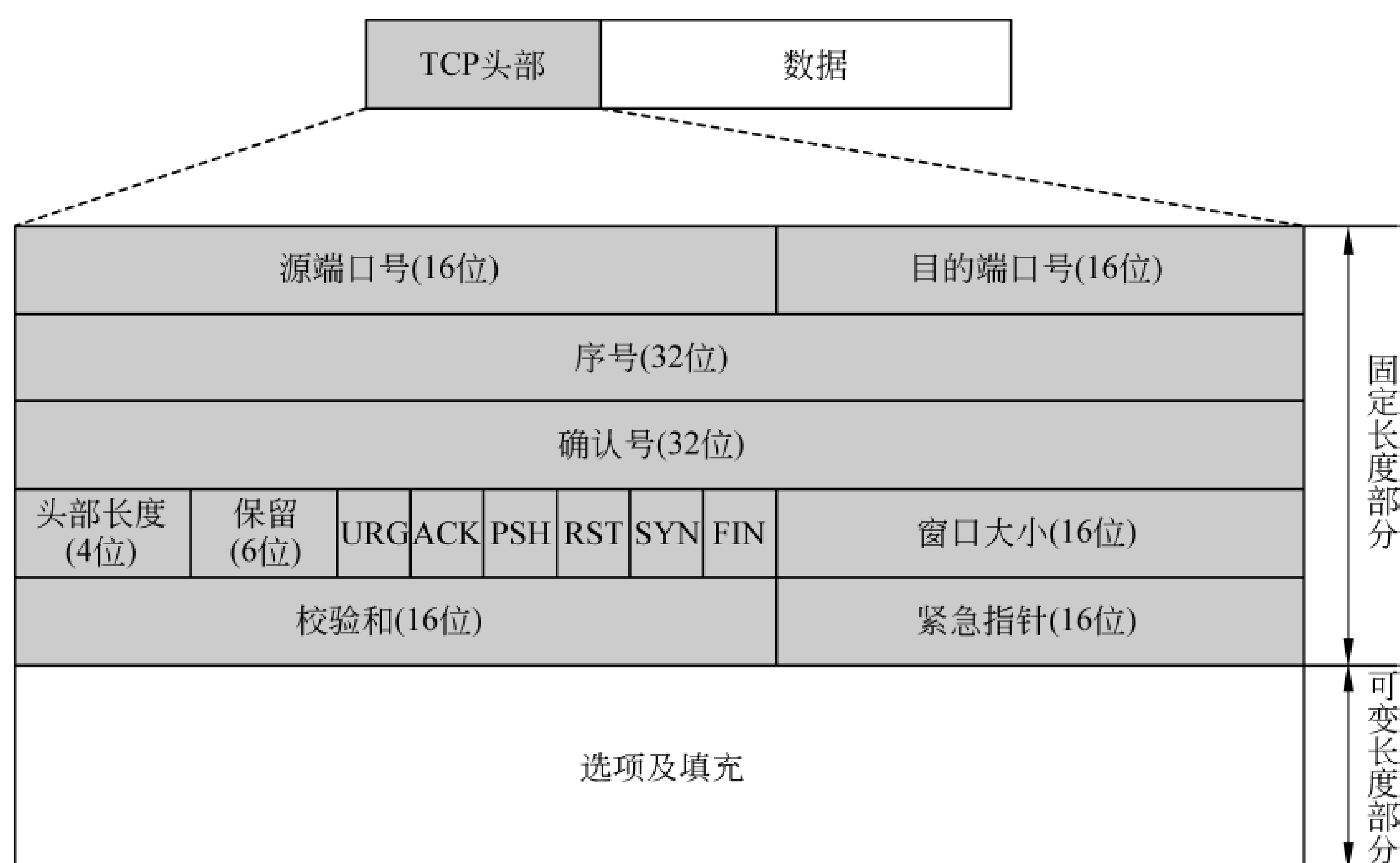


图 6-6　TCP 报文格式

ACK＝1。

② TCP 报文段序号对应第 25～32 字节的数据对应“序号”与“确认号”，十六进制值分别为：

seq＝e0 59 9f ef

ack＝84 6b 41 c6

- 编号 3 的数据：

① TCP 头部的 SYN 与 FIN 字段对应第 34 字节的数据。第 34 字节的数据为：10H，用十进制数表示为 16，用二进制表示为 0001 0110，对照在 TCP 报文头格式，为：SYN＝1，ACK＝1。

② TCP 报文段序号对应第 25～32 字节的数据对应“序号”与“确认号”，十六进制值分别为：

seq＝84 6b 41 c6

ack＝e0 59 9f f0

通过对编号 1 到编号 3 的 3 组数据的分析中可以看出，它们是主机 H 与服务器 S 建立 TCP 连接的三次握手的过程。

关于快速以太网(Fast Ethernet)填充问题的解答，要看封装到帧中 IP 分组的长度。Fast Ethernet 最小帧长度值与 Ethernet 相同，为 64B。

IP 分组的总长度值对应于表中第 3～4 个字段值。

第 1、2、4 分组的总长度值为 30H，即长度为 3×16B＝48B，大于 46B，不需要填充。

第 3、5 分组的总长度值为 28H，即长度为(2×16＋8)B＝40B，小于 46B，需要填充。

(3) 服务器已经接收到的应用层数据的字节数。

第 1、2、3 这 3 个报文段通过三次握手完成了主机 H 与服务器 S 的 TCP 连接。

第 4 报文段是主机 H 向服务器 S 发送数据，第 5 个报文段是服务器 S 向主机 H 发送确认。

第 3 报文段的序号为：

$$seq=84\ 6b\ 41\ c6$$

第 5 报文段的确认号为：

$$ack=84\ 6b\ 41\ d6$$

因此，服务器已经接收到的应用层数据长度为

$$84\ 6b\ 41\ d6-84\ 6b\ 41\ c6=10H=16B$$

（4）如果某个 IP 分组在服务器 S 发出时的前 40B 如表 6-5 所示，那么该 IP 分组到达主机 H 时，计算经过几个路由器。

表 6-5　S 发出的 IP 分组

S 发出的 IP 分组	45 00 00 28 68 11 40 00 40 06 ec ad d3 44 47 50 ca 76 01 06 13 88 a1 08 e0 59 9f f0 84 6b 41 d6 50 10 16 d0 b7 d6 00 00

为了回答这个问题，首先要确定表 6-5 与表 6-4 的服务器哪次发送的分组相关。这就要看分组的“标识”字段值。分组的“标识”字段值在表中对应第 5 和第 6 字节。

表 6-5 与表 6-4 中编号 5 的分组“标识”字段值都为“6811”。为了计算这个分组从服务器 S 发出到达主机 H 经过多少个路由器，只需要比较两个分组中的 TTL 值。TTL 值相应的位置是表中第 9 字节。

服务器 S 发出的 IP 分组

$$TTL=40H=4\times16=64$$

编号 5 的分组

$$TTL=31H=3\times16+1=49$$

那么，该分组经过的路由器数

$$n=64-49=15$$

答案：

（1）编号 1、3、4 的 IP 分组是由主机 H 发送给服务器 S 的。

编号 1、2、3 分组完成了 TCP 连接的三次握手。

编号为 3、5 的分组经过快速以太网发送时需要填充。

（2）服务器已经接收到的应用层数据长度为 16B。

（3）该分组经过 15 个路由器。

第三部分　综合练习——术语解析

从给出的 26 个定义中挑出 20 个，并将标识定义的字母填在对应术语前的空格位置。

（1）________熟知端口号　　（2）________端-端连接

（3）________ UDP　　（4）________伪报头

（5）________网络吞吐量　　（6）________饱和状态

（7）________死锁　　（8）________字节流

（9）________三次握手　　（10）________端口号

（11）________滑动窗口　　（12）________临时端口号

(13) ________套接字　　(14) ________保持计时器
(15) ________通知窗口　　(16) ________拥塞控制
(17) ________坚持计时器　　(18) ________传输实体
(19) ________四次握手　　(20) ________时间等待计时器

A. 路由器-路由器之间建立的连接。
B. 源主机进程与目的主机进程之间建立的连接。
C. 传输层中实现传输层协议的软件。
D. 标识不同进程的进程号。
E. 由 IP 地址与对应的进程号组成的标识。
F. 客户进程使用的进程标识。
G. 分配给标准的 Internet 服务的进程标识。
H. 网络环境中一个进程的全网唯一的标识。
I. 无连接的、不可靠的传输层协议。
J. UDP 校验和校验的对象除了原有报头之外增加的部分。
K. 功能完善的传输层协议。
L. TCP 协议传输应用程序数据时采取的形式。
M. TCP 连接建立的过程。
N. 客户端主动提出请求的连接释放的过程。
O. 为防止 TCP 连接处于长时期空闲而设置的计时器。
P. 为保证 TCP 连接释放过程正常进行而设置的计时器。
Q. 为控制报文确认与等待重传的时间而设置的计时器。
R. 为防止非零窗口通知丢失造成"死锁"现象而设置的计时器。
S. TCP 协议跟踪和记录发送字节的状态,实现差错控制功能的机制。
T. 用于流量控制的接收窗口的另一个名称。
U. 用于防止过多报文进入网络而造成路由器与链路过载现象的机制。
V. 当网络吞吐量的增长小于网络负载的增加量的现象。
W. 当网络负载增加而吞吐量不变的现象。
X. 当网络负载继续增加到一定程度,网络吞吐量为零的现象。
Y. 单位时间进入网络的字节数。
Z. 单位时间内通过网络输出的字节数。

参考答案:

(1) G	(2) B	(3) I	(4) J	(5) Z
(6) W	(7) X	(8) L	(9) M	(10) D
(11) S	(12) F	(13) E	(14) O	(15) T
(16) U	(17) R	(18) C	(19) N	(20) P

第 7 章

应用层

第一部分 同 步 练 习

7.1 Internet 应用发展与应用层协议的分类

7-1-1 以下关于客户/服务器模式比较的描述中，错误的是________。

A. 在一次进程通信中发起通信的一方叫作客户端，接收连接请求的一方叫作服务器端

B. 从工作模式角度，Internet 应用系统分为两类：客户/服务器模式与对等模式

C. 客户/服务器反映出这样一种网络服务提供者与网络服务使用者的关系

D. 所有程序在进程通信中的客户端与服务器端的地位是不变的

7-1-2 以下关于客户/服务器模式特点的描述中，错误的是________。

A. 每种服务器都能够安装一种特定的服务器程序

B. 安装服务器程序的主机作为服务器，为客户提供服务

C. 安装客户程序的主机作为客户端，是用户访问网络服务的用户界面

D. 在应用层的 C/S 工作模式中，服务器程序与客户程序是协同工作的两个部分

7-1-3 以下关于 P2P 应用程序体系结构特点的描述中，错误的是________。

A. 基于对等结构的 P2P 应用程序体系结构中所有节点的地位是平等的

B. 系统中不存在一直处于打开状态、等待客户服务请求的服务器

C. 在 P2P 应用程序进程通信中不存在客户/服务器模式问题

D. 每个节点既可以作为客户，又可以作为服务器

7-1-4 以下关于 P2P 与 C/S 模式区别与联系的描述中，错误的是________。

A. C/S 模式是以服务器为中心的

B. C/S 与 P2P 的差别主要在应用层和传输层

C. P2P 网络是一种在 IP 网络上构建的覆盖网

D. P2P 中所有节点同时是服务提供者与服务使用者

7-1-5 以下关于应用层协议的描述中，错误的是________。

A. 交换报文的端口号

B. 各种报文格式与包含的字段

C. 报文格式中每个字段意义的描述

D. 进程在什么时间、如何发送报文,以及如何响应

7-1-6 以下关于应用层体系结构的描述中,正确的是________。

A. 应用程序体系结构涉及应用程序功能、工作模型与协议结构

B. 在应用系统设计与研发时,设计者面对的是局域网环境

C. 设计者关心的是每条指令长度为多少个字节

D. 每条指令长度通过哪条路径传送到对方

7-1-7 请填写下面协议栈中缺少的主要协议名称。

	Web服务	网络管理服务	虚拟终端服务	电子邮件服务	动态主机地址分配服务	域名服务	文件传输服务
应用层							
传输层							
网络层							

7.2 域名系统DNS

7-2-1 以下关于DNS概念的描述中,错误的是________。

A. DNS使用统一的命名空间

B. DNS使用本地的缓存来改善系统的性能

C. DNS域名服务的处理依赖于所使用的传输系统

D. DNS数据库容量限制和更新频率都要求对域名进行分布式管理

7-2-2 以下关于DNS基本功能的描述中,错误的是________。

A. DNS要为用户提供一种能有效完成主机名与网络IP地址转换的机制

B. DNS必须提供一个所有可能出现的节点命名的名字空间

C. DNS必须为每台主机分配一个在全网具有唯一性的名字

D. DNS必须采取告知每个用户所有DNS的IP地址

7-2-3 以下关于域名空间、资源记录、域名服务器与地址解析程序关系的描述中,错误的是________。

A. 域名系统是由数量未知的域名服务器构成,每个域名服务器是域名空间树一部分

B. 域名空间是一个树型结构,用户可从该树的任何一处开始遍历

C. 地址解析程序将每个域名系统使用的数据库视为动态的数据库

D. 域名服务器可以对来自于地址解析程序的请求进行并行处理

7-2-4 以下关于DNS根域名服务器的描述中,错误的是________。

A. 目前存在13个DNS根域名服务器

B. a.root-server.net是一台DNS根域名服务器的域名

C. 根域名服务器都是位于一个地理位置的服务器集群组成

D. DNS根域名服务器对于DNS系统的整体运行具有极为重要的作用

7-2-5 以下关于域名解析工作原理的描述中,错误的是________。

A. 将域名转换为对应的IP地址的过程称为域名解析

B. 域名解析可以有两种方法：递归解析与反复解析

C. 递归解析要求名字服务器系统一次性完成全部名字-地址的变换

D. 递归解析的任务主要是由域名解析器软件完成

7.3 远程登录服务与 TELNET 协议

7-3-1 以下关于 TELNET 协议的描述中，错误的是________。

A. TELNET 协议的标准文档是于 1993 年完成并公布的

B. 不同型号计算机系统的差异性主要表现在硬件、软件与数据格式上

C. TELNET 协议引入了网络虚拟终端(NVT)的概念

D. 用户使用 TELNET 命令可以使自己计算机暂时成为远程计算机的仿真终端

7-3-2 以下关于 TELNET 工作原理的描述中，错误的是________。

A. 远程登录服务采用典型的客户/服务器模式

B. NVT 是一种统一的数据表示方式，以保证不同主机之间通信的兼容性

C. TELNET 进程完成用户终端格式、主机系统内部格式与标准 NVT 格式之间的转换

D. TELNET 只用于用户远程访问大型机

7.4 电子邮件服务与 SMTP 协议

7-4-1 以下关于邮件传输代理 MTA 与用户代理 UA 的描述中，错误的是________。

A. Internet 电子邮件系统将邮件工作系统与邮件的发送、接收系统分开

B. 邮件系统中存在邮件传输代理 MTA 与用户代理 UA

C. 接收方用户从用户代理 UA 中读取他的电子邮件

D. 中继 MTA 服务器在接收和发送邮件时都是作为服务器使用

7-4-2 以下关于电子邮件格式的描述中，错误的是________。

A. 电子邮件包括邮件头与邮件体两部分

B. 邮件头是由系统自动生成的发信人地址(From：)、邮件发送的日期与时间、收信人地址(To：)、抄送人地址(Cc：)与邮件主题(Subject：)等

C. 邮件体就是实际要传送的信函内容

D. MIME 协议允许电子邮件系统传输文字、图像、语音与视频等多种信息

7-4-3 以下关于邮件报文传送连接建立过程的描述中，错误的是________。

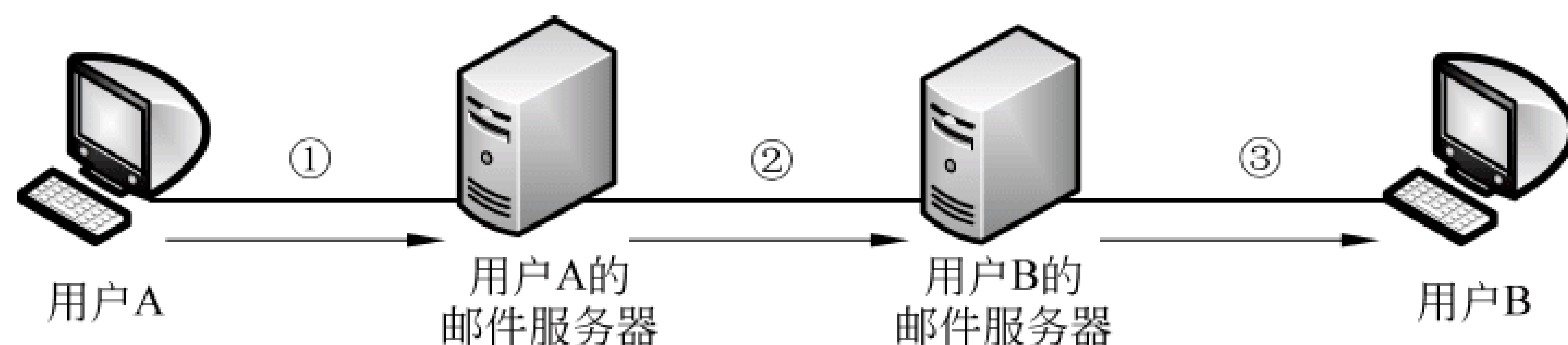
A. 客户用“MAIL FROM：wgy@nankai.edu.cn”向邮件服务器报告发信人邮箱与域名

B. 邮件服务器返回代码 250 表示请求命令完成，继续发送

C. 客户用“DATA”命令表示开始传送邮件主体

D. 客户用“RCPT TO”命令向服务器传送邮件

7-4-4 用户 A 与用户 B 的邮件系统结构与收发邮件过程如下图所示。



图中①、②、③依次表示网络中节点之间使用的邮件协议名称。以下给出的答案中正确的是________。

A. SMTP、SMTP、SMTP
B. SMTP、SMTP、POP3
C. SMTP、POP3、SMTP
D. POP3、SMTP、POP3

7-4-5 以下关于 MIME 协议特点的描述中,错误的是________。

A. SMTP 协议不支持多语种邮件的传输
B. SMTP 协议不支持语音、视频邮件的传输
C. MIME 是一种邮件传输协议
D. MIME 使用 NVT 标准,允许多语种邮件通过 SMTP 传输

7-4-6 以下关于 POP3 协议特点的描述中,错误的是________。

A. TCP 连接建立之后,才能建立 POP3 会话连接
B. 建立 POP3 会话连接过程中需要完成用户身份认证
C. 用户向服务器发出 RETR 请求,了解自己邮箱的状态
D. 删除邮件命令是在接收到"退出会话的 QUIT 命令"之后完成

7-4-7 以下关于 IMAP4 协议特点的描述中,错误的是________。

A. IMAP4 是一种邮件传输协议
B. 用户在下载邮件之前可以检查邮件的头部
C. 用户在下载邮件之前可以用特定的字符串搜索电子邮件的内容
D. 用户可以在邮件服务器上创建、删除邮箱,或对邮箱更名,创建分层次的邮箱

7-4-8 以下关于 Web 电子邮件的描述中,错误的是________。

A. 客户代理就是 Web 浏览器
B. 客户与远程邮箱之间通信使用 HTTP 协议
C. 客户与远程邮箱之间通信可以使用 POP3 或 IMAP 协议
D. 邮件服务器之间的通信仍然使用 SMTP 协议

7.5 Web 与基于 Web 的网络应用

7-5-1 以下关于主页概念的描述中,错误的是________。

A. 在 Web 环境中,信息以 Web 页的形式来显示与链接
B. Web 页是用 HTML 语言来实现,并在 Web 页之间建立超文本链接
C. 主页是指个人或机构基本的 Web 页
D. 主页一般包含 E-mail、SNMP 与 NNTP 等信息

7-5-2 当用户在 Web 浏览器中输入域名 www. nankai. edi. cn 访问学校网站时,浏览器可能发送哪几个报文?

7-5-3 以下关于 HTTP 协议特点的描述中,错误的是________。

A. HTTP 在传输层使用的 TCP 协议
B. Web 浏览器想访问一个 Web 服务器,就需要在两个进程之间建立一个 TCP 连接

C. Web 浏览器进程通过套接字发送 HTTP 请求报文，Web 服务器发送应答报文

D. 如果传输的请求与应答报文丢失，将由 Web 浏览器与 Web 服务器组织重发

7-5-4 以下关于 HTTP 非持续连接特点的描述中，错误的是________。

A. HTTP 协议支持非持续连接与持续连接

B. HTTP/1.0 版协议定义非持续连接，而 HTTP/1.1 默认状态为持续连接

C. 非持续连接中对每次请求/响应都要建立一次 TCP 连接

D. 非持续连接中读取 100 张图片，那么需要打开与关闭 100 次 TCP 连接

7-5-5 估算非持续连接工作模式请求一个 HTTP 文件所需的时间。

条件：

(1) 测试的 RTT 的平均值为 1500ms，传输一个 gif 文件时间平均为 3500ms。

(2) 一个 Web 页中有 85 个 gif 文件。

要求：

(1) 采用串行方法获取 85 个 gif 文件所需的时间。

(2) 采用并行方法(每次连接获取 10 个 gif 文件)获取 85 个 gif 文件所需的时间。

7-5-6 以下关于 HTTP/1.0 协议持续连接的描述中，错误的是________。

A. 在持续连接时，Web 服务器在发出响应后保持该 TCP 连接

B. 一个包括 1 个基本 HTLM 文件和多个 JPEG 图形文件的完整 Web 页可以通过一个持续的 TCP 连接来传送

C. 一个 Web 服务器中的多个 Web 页要通过多个持续的 TCP 连接来传送

D. Web 服务器在接收到用户机的请求或超时才关闭该连接

7-5-7 以下关于 Web 文档类型的描述中，错误的是________。

A. Web 文档分为 3 种类型：静态文档、动态文档与活动文档

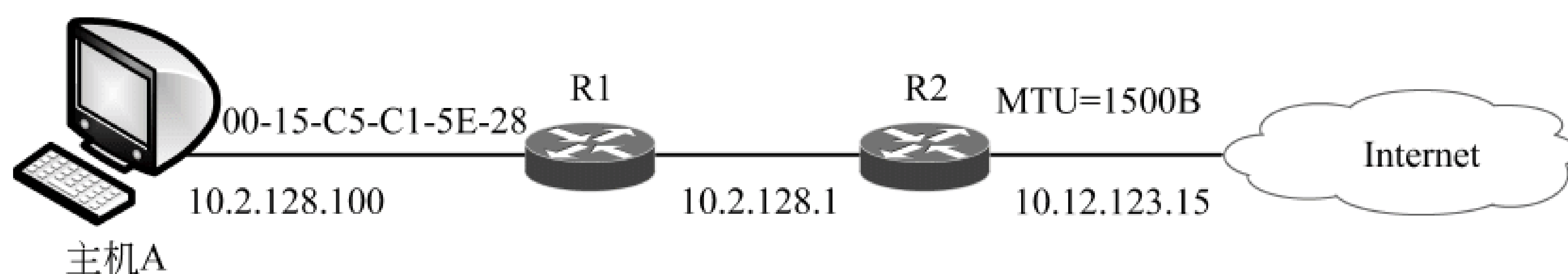
B. 静态文档是由服务器创建和保存，内容固定的文档

C. 浏览器在用户端计算机中运行程序产生动态文档

D. 活动文档是一种二进制代码形式的文档

7-5-8 一个 Web 网站有 1×10^7 个网页，平均每个网页有 10 个链接。读一个网页平均需要 100ms。问：检索整个网站最少需要多少时间？

7-5-9 网络拓扑如下图所示。主机 A 的 MAC 地址是 00-15-C5-C1-5E-28，IP 地址为 10.2.128.100。



下表是 Ethernet 帧前 80B 的十六进制数。

0000	00	21	27	21	51	ee	00	15	c5	c1	5e	28	08	00	45	00
0010	01	ef	11	3b	40	00	80	06	ba	9d	0a	02	80	64	40	aa
0020	62	20	04	ff	00	50	e0	e2	00	fa	7b	f9	f8	05	50	18
0030	fa	f0	1a	c4	00	00	47	45	54	20	2f	72	66	63	2e	68
0040	74	6d	6c	20	48	54	54	50	2f	31	2e	31	0d	0a	41	63

回答以下问题:

(1) Web服务器的IP地址是什么? 主机A的默认网关MAC地址是什么?

(2) 主机A在构造表中所示的数据帧时,使用什么样的协议去确定目的MAC地址的? 封装该协议请求报文的Ethernet帧的目的地址是什么?

(3) 假设HTTP/1.1协议以持续的非流水线方式工作,一次"请求-响应"时间是RTT。Rfc.html页面引用了5个JPEG小图像,则从图中所示Web请求开始到浏览器收到全部内容为止,需要多少个RTT?

(4) 该帧所封装的IP分组经过路由器转发时,需要修改IP分组头的哪些字段?

7.6 即时通信与SIP协议

7-6-1 以下关于即时通信工作模型的描述中,错误的是________。

A. 即时通信工作模型可以分为在线的对等通信方式与离线的中转通信方式

B. QQ属于分布式P2P结构

C. QQ用户需要在QQ服务器上注册,并获得自己的用户名与密码

D. 在登录成功后,QQ用户可以通过服务器下载自己的好友列表、在线或离线信息

7-6-2 以下关于SIP协议的描述中,错误的是________。

A. SIP是在传输层实现即时通信的控制信令协议

B. SIP中的"会话"是指用户之间的数据传输

C. SIP采用了用户/服务器工作模式

D. sip:wugongyi@nankai.edu.cn是一种SIP地址

7-6-3 以下关于SIP协议工作模式的描述中,错误的是________。

A. SIP协议定义了用户代理与网络服务器

B. 用户代理包括用户代理客户与用户代理服务器

C. 用户代理客户发起呼叫,而用户代理客户则接受呼叫

D. 用户代理客户是笔记本计算机、PDA或移动电话等硬件设备

7-6-4 以下关于SIP网络服务器的描述中,错误的是________。

A. 重定向服务器不接受SIP呼叫路由,只处理用户呼叫请求

B. 注册服务器保存用户地址与当前所在位置的映射关系

C. 代理服务器分为有状态代理与无状态代理

D. 代理服务器也称为"SIP路由器"

7.7 主机配置与动态主机配置协议DHCP

7-7-1 以下关于主机配置与DHCP协议的描述中,错误的是________。

A. 主机配置参数主要有网络默认路由器地址、掩码、服务器地址、分组TTL值等

B. 对于远程主机、移动设备、无盘工作站和地址共享的配置,可以手工完成

C. 在TCP/IP协议体系中,DHCP协议位于网络层

D. DHCP可以为主机自动分配IP地址及其他一些重要参数

7-7-2 以下关于DHCP服务器功能的描述中,错误的是________。

A. IP地址储存与管理　　B. DNS服务器请求响应

C. 租用管理与服务管理　　D. 配置参数的存储和管理

7-7-3 以下关于 DHCP 客户功能的描述中，错误的是________。

A. 发起配置　　B. 租用管理　　C. 配置参数管理　　D. TCP 报文重传

7-7-4 以下关于 DHCP 客户与服务器交互过程的描述中，错误的是________。

A. 客户端租用请求报文是以点-点方式发送出去的

B. 接收到客户端请求报文的服务器都要返回一个应答报文

C. 租用应答报文包括分配给客户的 IP 地址、租用期与参数

D. 客户与被选择的服务需要再次进行请求与应答报文的交互

7-7-5 以下关于 DHCP 租用信息的描述中，错误的是________。

A. 用租用的方式将 IP 地址动态地分配给主机

B. 将 IP 地址与主机的 MAC 地址绑定

C. 服务器管理 IP 地址的租用期

D. 租用期的单位为小时

7-7-6 下表为某 DHCP 用户执行 ipconfig/all 命令时得到的部分信息。

```
Ethernet adapter 本地连接：
  Connection-specific DNS suffix.:
  Description………… : Broadcom 440X 10/100 Integrated Controller
  Physical  Address……: 2A2200110090
  DHCP Enabled………: Yes
  IP Address……………: 211.1.1.3
  Subnet Mask…………: 255.255.255.0
  Default Gateway……:  211.1.1.1
  DHCP Server………:  211.1.1.5
  Lease Obtained……:  2011.3.10  8:25:00
  Lease Expires……:   2011.3.16  8:25:00
```

下图为在依次执行 ipconfig/release 与 ipconfig/renew 时获取的报文，以及对第 5 条报文解析的结果。请根据你对 DHCP 工作原理的理解，填充①～⑤的信息。

Sniffer Portable - Local, Ethernet (Line speed at 100 Mbps) - [a2.cap: Filtered 3, 36/25000 Ethernet Frames, Filter: Matrix]

File Monitor Capture Display Tools Database Window Help

No	Source Addes	Dest. Addes	Summary
1	①	②	DHCP:Reply,Type: ③
2	201.1.1.5	255.255.255.255	DHCP:Request,Type:DHCP offer
3	0.0.0.0	255.255.255.255	DHCP:Reply,Type:DHCP request
4	201.1.1.5	④	DHCP:Reply,Type: ⑤

```
DHCP:------DHCP Header------
      DHCP:Boot record type                    =2(Reply)
      DHCP:Hardware address type               =1(10Mbps Ethernet)
      DHCP:Hardware address length             =6 bytes
      DHCP:Client self-assigned address        =[0.0.0.0]
      DHCP:Client address                      =201.1.3
      DHCP:Next server to use in bootstrap     =[0.0.0.0]
      DHCP:Relay  agent                        =[0.0.0.0]
      DHCP:Client hardware address             =2A2200110090
      DHCP:Message type                        =5(DHCP Ack)
      DHCP:Address renewel interval            =34560(seconds)
      DHCP:Address rebinding interval          =604800(seconds)
      DHCP:Request IP Address Lease time       =61200(seconds)
      DHCP:Subnet mask                         =255.255.255.240
      DHCP:Gateway address                     =201.1.1.1
      DHCP:DNS address                         =201.1.10.10
```

7-7-7 下图是 DHCP 客户机捕获的报文，并对第 4 个报文进行了解析。请根据图中提供的

信息,回答以下问题。

Sniffer Portable - Local, Ethernet (Line speed at 100 Mbps) - [a2.cap: Filtered 3, 36/25030 Ethernet Frames, Filter: Matrix]

File Monitor Capture Display Tools Database Window Help

Default

No	Source Addes	Dest. Addes	Summary
1	0.0.0.0	255.255.255.255	DHCP：Request，Type：DHCP discover
2	211.80.20.1	255.255.255.255	DHCP：Request，Type：DHCP offer
3	0.0.0.0	255.255.255.255	DHCP：Request，Type：DHCP Request
4	211.80.20.1	255.255.255.255	DHCP：Reply，Type：DHCP ack

```
DHCP:………………DHCP Header…………………
    DHCP:Boot record type                  =2(Reply)
    …………
    DHCP:Client self-assigned address      =[0.0.0.0]
    DHCP:Client address                    =[211.80.20.120]
    DHCP:Next Server to use  in bootstrap  =[0.0.0.0]
    DHCP:Replay Agent                      =[0.0.0.0]
    DHCP:Client hardware address           =05F1224500F6
    ……
    DHCP:Vendor Infrmation tag             =63825363
    DHCP:Message Type                      =5(DHCP ack)
    DHCP:Address renewel interval          =345600(seconds)
    DHCP:Address rebinding interval        =604800(seconds)
    DHCP:Request IP Address Lease time     =691200(seconds)
    DHCP:Subnet mask                       =255.255.255.240
    DHCP:Gateway address                   =[211.80.20.2]
    DHCP:Domain Name Server address        =[211.25.110.8]
```

(1) 客户机从 DHCP 获得的 IP 地址是什么? 客户机的 MAC 地址是什么?

(2) 在 DHCP 服务器中设置的 DNS 服务器的 IP 地址是什么? 路由器的 IP 地址是什么?

(3) DHCP 服务器的 IP 地址是什么?

7.8 网络管理与 SNMP 协议

7-8-1 以下关于网络管理概念的描述中,错误的是________。

A. 网络管理是对网络资源有效利用,网络故障时及时报告和处理,网络正常运行

B. 网络管理系统由管理进程、被管对象、代理进程、管理信息库组成

C. 每个代理进程管理自己的本地 MIB,并与管理进程交换网络状态信息

D. 多个本地 MIB 共同构成整个网络的 MIB

7-8-2 以下关于 SNMP 协议的描述中,错误的是________。

A. SNMP 由两部分内容组成:SNMP 体系结构与 SNMP 协议

B. 当一个网络资源不能与管理进程直接交换管理信息时,就需要使用外部代理

C. 外部代理按照 SNMP 协议与网络管理进程通信,还要与被管理的网络设备通信

D. SNMP 在传输层采用 TCP 协议

7-8-3 以下关于 SNMP 基本操作的描述中,错误的是________。

A. 采用周期性轮询的方式

B. 通过“读”、“写”两种操作来实现基本的网络管理功能

C. 使用 Set 报文来改变代理进程状态

D. 使用 Get 报文检测被管对象状态

7-8-4 根据 SNMP 协议被管对象命名方法,如果一个公司准备向市场推出它们新研制的一款服务器产品。假设公司在 enterprise 的子树之下有一个 MIB 节点号 150,它是为新款服务器产品申请了标识符编号为 50。请写出服务器对象标识符编码。

7.9 典型应用层协议——FTP 的分析

7-9-1 以下关于 FTP 用户程序特点的描述中，错误的是________。
A. FTP 用户程序主要有传统的 FTP 命令行、浏览器与 FTP 下载工具
B. 传统的 FTP 命令行是最早的 FTP 用户程序
C. 浏览器软件支持访问 FTP 服务器，可以直接登录到 FTP 服务器并下载文件
D. 使用 FTP 命令行从 FTP 服务器下载文件的过程中出现网络连接意外中断，用户程序通过断点续传功能可以继续进行剩余部分的传输

7-9-2 以下关于 FTP 工作模型的描述中，错误的是________。
A. FTP 协议使用控制连接、数据连接来完成文件的传输
B. 用于控制连接的 FTP 服务器端使用的熟知端口号为 21
C. 用于控制连接的 FTP 客户端使用的端口号为 20
D. FTP 服务器端包括两个部分：控制进程、数据进程

第二部分 同步练习答案与解析

7.1 Internet 应用发展与应用层协议的分类

7-1-1 分析：设计该例题的目的是加深读者对客户/服务器模式与 P2P 网络工作模式的理解。在讨论客户/服务器工作模式时，需要注意以下几个主要问题：

（1）从工作模式的角度，Internet 应用系统可以分为两类：客户/服务器（C/S）模式与对等（P2P）模式。

（2）术语 C/S 经常在两种情况出现：

① 从传输层分布式进程通信实现方法的角度，在一次进程通信中请求连接、发起通信的一方叫做客户（client）端，而接收连接建立请求、提供网络服务的一方叫做服务器（server）端。

② 从应用层的网络服务实现技术的角度，网络节点可以分为两类：客户和服务器。普通的网络客户通过作为“客户（client）”的计算机向服务器请求一种网络服务。网络“服务器（server）”为客户提供服务。读者通过 Web 浏览器去访问一个 Web 服务器时，读者的计算机就是一个“客户”，被访问的、存储 Web 页的计算机就是一个“服务器”。

（3）Internet 应用系统采用 C/S 模式的主要原因是：网络资源分布的不均匀性。网络资源分布的不均匀性表现在硬件、软件和数据。

① 网络中计算机系统的类型、硬件结构、功能都存在着很大的差异。它可以是一台大型计算机、高档服务器，也可以是一台个人计算机，甚至是一个 PDA 或者是一个家用电器。它们在运算能力、存储能力和外部设备的配备等方面存在着非常大的差异。

② 从软件的角度看，很多大型应用软件都是安装在一台专用的服务器中，客户需要通过 Internet 去访问服务器，成为合法客户，来共享软件资源。

③ 从信息资源的角度，某些数据、文本、图像、视频或音乐资源存放在一台或几台大型服务器中，其他合法客户可以通过 Internet 去访问这些信息资源。这样做对保证信息资源使用的合法性、安全性，以及保证数据的完整性与一致性是非常必要的。

(4) 客户/服务器反映出这样一种网络服务提供者与网络服务使用者的关系。在客户/服务器模式中,客户与服务器在网络服务中的地位是不平等的,服务器在网络服务中处于中心地位。

设计这个例题是因为客户/服务器(C/S)是一个经常引起歧义的术语。术语C/S经常在两种情况出现:一是从传输层分布式进程通信实现方法的角度,二是从应用层网络服务实现技术的角度。从传输层分布式进程通信实现方法的角度,在一次进程通信中请求连接、发起通信的一方叫做客户(client)端,而接收连接建立请求、提供网络服务的一方叫做服务器(server)端。那么,客户端与服务器端是与一次进程通信相关,凡是提出进程通信请求的一方就是客户端,而接收请求的一方就是服务器端,因此对于不同的程序,它既可以成为客户端,也可以成为服务器端。Internet应用系统的服务器计算机与客户计算机的地位确实是不变的,一方是提供服务,另一方是请求服务。

因此,D对进程通信的描述是错误的。

答案:D。

7-1-2 分析:设计该例题的目的是加深读者对应用层客户/服务器工作模式特点的理解。在讨论应用层C/S工作模式时,需要注意以下几个主要问题:

(1) 服务器程序与服务器。

在应用层C/S工作模式中,作为端系统的计算机可以分为客户端与服务器端。服务器程序与客户程序是协同工作的两个部分。在Internet的很多网络应用(如FTP、E-mail、Web)中,服务器应用程序运行在一台高配置计算机中,这台计算机专门提供一种或几种网络服务功能。

(2) C/S工作模式具有以下几个特点:

① 服务器程序在固定的IP地址和熟知的端口号上一直处于打开状态,随时准备接收客户端的服务请求。客户端程序可以根据客户需要,在访问服务器时打开。

② 客户端之间不能够直接通信。

③ 当同时向服务器发出服务请求的客户数量比较多时,一台服务器不能够满足多个客户请求的需要。人们经常使用由多台服务器组成的服务器集群(server cluster)去构成一个虚拟服务器。同时,在客户数量比较少,或者是客户服务请求不频繁的情况下,也可以将多种服务器应用程序安装在一台计算机中。一台服务器就可以提供多种网络服务功能。

因此,A对“每种服务器都能安装一种特定的服务器程序”的描述是不准确的。

答案:A。

7-1-3 分析:设计该例题的目的是加深读者对P2P应用程序体系结构特点的理解。在讨论P2P应用程序体系结构的特点时,需要注意以下几个主要问题:

(1) 如果将基于对等结构的P2P应用程序体系结构与基于C/S应用程序体系结构比较,P2P应用程序体系结构中所有节点的地位是平等的,系统中不存在一直处于打开状态、等待客户服务请求的服务器。

(2) P2P应用程序体系结构中每个节点都可以既是发出信息共享请求的客户,又可以是为其他对等节点提供共享信息的服务器。

(3) 如果从进程间相互作用工作模式的角度,在一对采用对等方式通信的应用进程中,发出服务请求的一方仍然是客户端,而响应请求的进程仍然是服务器端。这点不会有改变。

(4) 实际上,在一些 P2P 文件共享系统中,一个进程既能够上传文件同时又能够下载文件,那么在上传文件与下载文件的两个会话连接中,仍然可以根据进程的发起与响应来区别出客户端与服务器端。

因此,C 的描述是错误的。

答案:C。

7-1-4 分析:设计该例题的目的是加深读者对 P2P 与 C/S 工作模式的区别与联系的理解。在讨论 P2P 与 C/S 工作模式的区别与联系时,需要注意以下几个主要问题:

(1) 传统的 Internet 中信息资源的共享是以服务器为中心的 C/S 工作模式,服务提供者与服务使用者之间的界限是很清晰的。

(2) P2P 网络则是淡化了服务提供者与服务使用者的界限,所有用户同时身兼服务提供者与服务使用者的双重身份。

(3) 在 P2P 网络环境中,成千上万台计算机之间处于一种对等的地位,整个网络一般不依赖于专用的集中式服务器。

(4) P2P 网络中的每台计算机既可以作为网络服务的使用者,也可以向其他提出服务请求的用户提供资源和服务。这些资源可以是数据资源、存储资源或计算资源等。

(5) 传统 Internet 的 C/S 模式与 P2P 模式在传输层及以下各层的协议结构是相同的,差别在应用层。

(6) P2P 网络并不是一个新的网络结构,而是一种新的网络应用模式。构成 P2P 网络的节点一般已经是 Internet 节点,它们脱离了传统的 Internet 基于客户/服务器的工作模式,不依赖于网络服务器,在 P2P 应用软件的支持下以对等方式共享资源与服务,在 IP 网络上形成一个逻辑的网络。P2P 网络是一种在 IP 网络上构建的覆盖网。

从以上讨论中可以看出,C/S 模式与 P2P 模式在传输层及以下各层的协议结构是相同的,差别就在应用层。因此,B 的描述是错误的。

答案:B。

7-1-5 分析:设计这道习题的目的是希望加深读者对应用层协议基本内容的理解。

应用层协议定义了运行在不同端系统上应用程序进程交换的报文格式与交互过程,它主要包括:

(1) 交换报文的类型,如请求报文与应答报文。

(2) 各种报文格式与包含的字段。

(3) 报文格式中每个字段含义的描述。

(4) 进程在什么时间、如何发送报文,以及如何响应。

因此,A 的描述是错误的。

答案:A。

7-1-6 设计这道习题的目的是希望加深读者对应用层体系结构基本概念的理解。

(1) 在实际开展一项 Internet 应用系统设计与研发任务时,设计者面对的不会只是单一的广域网或局域网环境,而将是多个由路由器互联起来的局域网、城域网与广域网构成的、复杂的 Internet 环境。

(2) 在设计这种基于 Internet 的分布式计算软件系统时,设计者关心的是协同计算的功能是如何实现的,而不是每条指令或数据具体是以长度为多少字节的分组,以及通过哪条

路径传送到对方的。

(3) 面对被抽象为边缘部分与核心交换部分的 Internet,网络应用系统设计工程师在设计一种新的网络应用时,他只需要考虑如何利用核心交换部分所能提供的服务,而不必涉及核心交换部分的路由器、交换机等低层设备或通信协议软件的编程问题。他的注意力可以集中到运行在多个端系统之上的网络应用系统功能、工作模型的设计与应用软件编程上,这就使得网络应用系统的设计开发过程变得更加容易和规范。这点也体现了网络分层结构的基本思想,也反映出网络技术的成熟。

(4) 网络应用程序功能、工作模型与协议结构定义为应用程序体系结构(Application Architecture)

因此,A 的描述是正确的。

答案:A。

7-1-7 分析:设计这道习题的目的是帮助读者加深对应用层协议综合知识的了解。

答案:

	Web服务	网络管理服务	虚拟终端服务	电子邮件服务	动态主机地址分配服务	域名服务	文件传输服务
应用层	HTTP	SNMP	TELNET	SMTP	DHCP	DNS	FTP
传输层	TCP	UDP	TCP	TCP	TCP	UDP	TCP
网络层	IP	IP	IP	IP	IP	IP	IP

7.2 域名系统 DNS

7-2-1 分析:设计该例题的目的是加深读者对 DNS 概念的理解。DNS 的设计目标为:

(1) 使用统一的命名空间。为了避免因特殊编码而引起的问题,域名中不能使用如网络标识符、地址、路由或类似信息作为名字的组成部分。

(2) 数据库容量限制和更新频率都要求对域名进行分布式管理,并使用本地的缓存来改善系统的性能。

(3) DNS 具有通用性,必须适应各种应用需求,要适应可能出现的各种新的服务。

(4) 域名服务的处理必须独立于它所使用的传输系统。

(5) DNS 必须适应于各类主机环境。

因此,C 关于 DNS 域名服务处理与传输系统关系的描述是错误的。

答案:C。

7-2-2 分析:设计该例题的目的是加深读者对 DNS 基本功能的理解。DNS 必须具备的基本功能是:名字空间定义、名字注册与名字解析。

(1) 名字空间定义必须提供一个所有可能出现的节点命名的名字空间。

(2) 名字注册必须为每台主机分配一个在全网具有唯一性的名字。

(3) 名字解析要为用户提供一种能有效完成主机名与网络 IP 地址转换的机制。

从以上分析中可以看出,D 关于"DNS 必须采取告知每个用户所有 DNS 的 IP 地址"的描述是不正确的。

答案:D。

7-2-3 分析：设计该例题的目的是加深读者对域名空间和资源记录、域名服务器与地址解析程序的关系的理解。在讨论域名空间和资源记录、域名服务器与地址解析程序的关系时，需要注意以下几个主要问题：

(1) 用户可以通过本地地址解析程序的简单的过程调用或系统调用，对域名系统进行访问。由于域名空间是一个树形结构，因此用户可以从该树的任何一处开始遍历。

(2) 从地址解析程序的角度看，域名系统则是由数量未知的域名服务器构成的系统，每个域名服务器只带有整个域名空间树数据的一部分，但地址解析程序将每个域名系统使用的数据库视为基本的静态数据库。

(3) 从域名服务器的角度看，域名系统是由相互独立的称为"区域"的本地数据集构成。域名服务器对一些区域有本地备份。域名系统下的域名服务器必须周期性用来自于本地或外部的域名服务器的主备份文件，对本地的区域数据进行刷新。域名服务器必须对来自于地址解析程序的请求进行并行处理。

从以上分析中可以看出，C 对每个域名系统使用数据库的描述是错误的。

答案：C。

7-2-4 分析：设计该例题的目的是加深读者对 DNS 根域名服务器特点的理解。在讨论 DNS 根域名服务器时，需要注意以下几个主要问题：

(1) DNS 在名字空间、注册权威机构的设立、域名服务器的设置都遵循了层次结构的概念，而 DNS 根域名服务器对于 DNS 系统的整体运行具有极为重要的作用。

(2) 任何原因造成根域名服务器停止运转，都会导致整个 DNS 系统的关闭，因此出于安全的原因，DNS 根域名服务器不可能只有一台。目前，存在 13 个 DNS 根域名服务器。

(3) 在专用域 root-server. net 之下，以字母 a～m 开始的 13 个根域名服务器，例如 a. root-server. net～mroot-server. net 等。

(4) 大多数根域名服务器都是由独立的多台物理的服务器构成的服务器集群组成。有些根域名服务器则是由分布在不同地理位置的多台镜像 DNS 服务器组成的。

从以上的分析中可以看出，C 对"根域名服务器都是位于一个地理位置的服务器集群组成"的描述是错误的。

答案：C。

7-2-5 分析：设计该例题的目的是加深读者对域名解析工作原理的理解。在讨论域名解析的工作原理时，需要注意以下几个主要问题：

(1) 将域名转换为对应的 IP 地址的过程称为域名解析。

(2) 完成该功能的软件叫做域名解析器软件。

(3) 用户在进行查询时，首先向域名服务器发出一个带有待解析的 DNS 请求(DNS request)报文。

(4) 域名解析可以有两种方法：递归解析与反复解析。

(5) 递归解析要求名字服务器系统一次性完成全部名字-地址变换。

(6) 反复解析是每次请求一个服务器，如果不行，再请求别的服务器。

(7) 两者的主要区别是：递归解析的任务主要是由服务器软件承担，而反复解析的任务主要是由域名解析器软件承担。

从以上分析中可以看出，D 对负责解析算法主体的描述是错误的。

答案：D。

7.3 远程登录服务与TELNET协议

7-3-1 分析：设计该例题的目的是加深读者对TELNET协议的理解。在讨论TELNET协议时，需要注意以下几个主要问题：

(1) RFC854是TELNET协议的标准文档，它是于1983年5月完成并公布的。

(2) 不同型号计算机系统的差异性主要表现在硬件、软件与数据格式上。最基本的问题是：不同计算机系统对终端键盘输入命令的解释不同。

(3) 为了解决异构计算机系统互联中存在的问题，人们研究TELNET协议。TELNET协议引入网络虚拟终端(Network Virtual Terminal，NVT)的概念，它提供一种专门的键盘定义，用来屏蔽不同计算机系统对键盘输入的差异性，同时定义用户与远程服务器之间的交互过程。TELNET协议的优点是能解决不同类型的计算机系统之间的互操作问题。远程登录服务是指用户使用TELNET命令，使自己的计算机暂时成为远程计算机的一个仿真终端的过程。一旦用户成功地实现远程登录，用户计算机就可以像一台与远程计算机直接相连的本地终端一样工作。因此，TELNET协议又称为网络虚拟终端协议、终端仿真协议或远程终端协议。

从以上分析中可以看出，A关于TELNET协议出现时间的描述是错误的。

答案：A。

7-3-2 分析：设计该例题的目的是加深读者对TELNET工作原理的理解。在讨论TELNET的工作原理时，需要注意以下几个主要问题：

(1) TELNET已经成为TCP/IP协议集中的一个基本协议。E-Mail、FTP与Web服务都是建立在TELNET NVT的基础上。

(2) 远程登录服务采用典型的用户/服务器模式。

(3) 用户的实终端(real terminal)采用用户终端格式与本地TELNET用户通信；远程计算机采用主机系统格式与TELNET服务器通信。在TELNET用户进程与TELNET服务器进程之间，通过网络虚拟终端(NVT)标准来进行通信。

(4) NVT是一种统一的数据表示方式，以保证不同硬件、软件与数据格式的终端与主机之间通信的兼容性。

(5) 引入网络虚拟终端概念之后，不同的用户终端与服务器进程将与各种不同的本地终端格式无关。TELNET用户与服务器进程完成用户终端格式、主机系统内部格式与标准NVT格式之间的转换。

从以上分析中可以看出，D关于TELNET应用领域的描述是错误的。

答案：D。

7.4 电子邮件服务与SMTP协议

7-4-1 分析：设计该例题的目的是加深读者对邮件传输代理MTA与用户代理UA概念的理解。在讨论MTA与UA的概念时，需要注意以下几个主要问题：

(1) 为了使系统运行效率最高，Internet电子邮件系统首先是将邮件工作系统与邮件发送、接收系统分开。

(2) 邮件系统通常为用户分别提供两个服务：一个是负责在 Internet 上传送邮件的邮件传输代理(MTA)，另一个是为用户提供阅读、编辑以及管理邮件的用户端应用，即用户代理(UA)。

(3) 用户端的邮件传输代理 MTA 接收待发送的邮件，将它通过 Internet 发送出去；服务器端的邮件传输代理 MTA 接收邮件，并将它发送给接收端用户代理 UA。

(4) 用户代理 UA 为用户提供一种对邮件进行编辑、阅读、发送、存储及管理的工具。接收端用户从用户代理 UA 中读取他的电子邮件。

(5) 在实际的电子邮件系统中，发送端用户需要通过多个中继 MTA 服务器，存储转发邮件。中继 MTA 服务器在接收邮件时是作为服务器，在发送邮件时又是作为用户。

从以上分析中可以看出，D 关于中继 MTA 服务器在接收和发送邮件作用的描述是错误的。

答案：D。

7-4-2 分析：设计该例题的目的是加深读者对电子邮件格式的理解。在讨论电子邮件的格式时，需要注意以下几个主要问题：

(1) 电子邮件包括邮件头(mail header)与邮件体(mail body)两部分。

(2) 邮件头是由多项内容构成，其中一部分是由系统自动生成，如发信人地址(From：)、邮件发送的日期与时间；另一部分是由发件人输入，如收信人地址(To：)、抄送人地址(Cc：)与邮件主题(Subject：)等。

(3) 邮件体就是实际要传送的信函内容。传统的电子邮件系统只能传输英文信息，而采用 MIME 的电子邮件系统可以传输文字、图像、语音与视频等多种信息。

从以上分析中可以看出，邮件头是由系统自动生成的发信人地址(From：)、邮件发送的日期与时间，而收信人地址(To：)、抄送人地址(Cc：)与邮件主题(Subject：)等内容由用户输入。因此，B 的描述是错误的。

答案：B。

7-4-3 分析：设计该例题的目的是加深读者对邮件报文传送过程的理解。在讨论邮件报文传送过程时，需要注意以下几个主要问题：

(1) 在 SMTP 客户与服务器之间的连接建立之后，发信的用户就可以与一个或多个收信人交换报文。

(2) 典型的报文传送过程为：

- 用户用“MAIL FROM：wgy@nankai.edu.cn”向服务器报告发信人的邮箱与域名。
- 服务器向用户发“250”(请求命令完成)的响应。
- 用户用“RCPT TO”命令向服务器报告收信人的邮箱与域名。
- 服务器向用户发“250”(请求命令完成)的响应。
- 用户用“DATA”命令对报文的传送进行初始化。
- 服务器向用户发“354”(开始邮件输入)的响应。
- 用户用连续的行向服务器传输报文的内容，每行以二字符的行结束标记(回车和换行)终止。报文以只有一个“.”的行结束。
- 服务器向用户发“250”(请求命令完成)的响应。
- SMTP 应答中规定：220 表示“服务就绪”，而 250 表示“请求命令完成”。

因此,D关于“用户用RCPT TO命令向服务器传送邮件”是错误的。

答案:D。

7-4-4 分析:设计这道题目的目的是帮助读者理解电子邮件系统协议的用途。

用户A与用户B的邮件系统结构如图7-1所示。

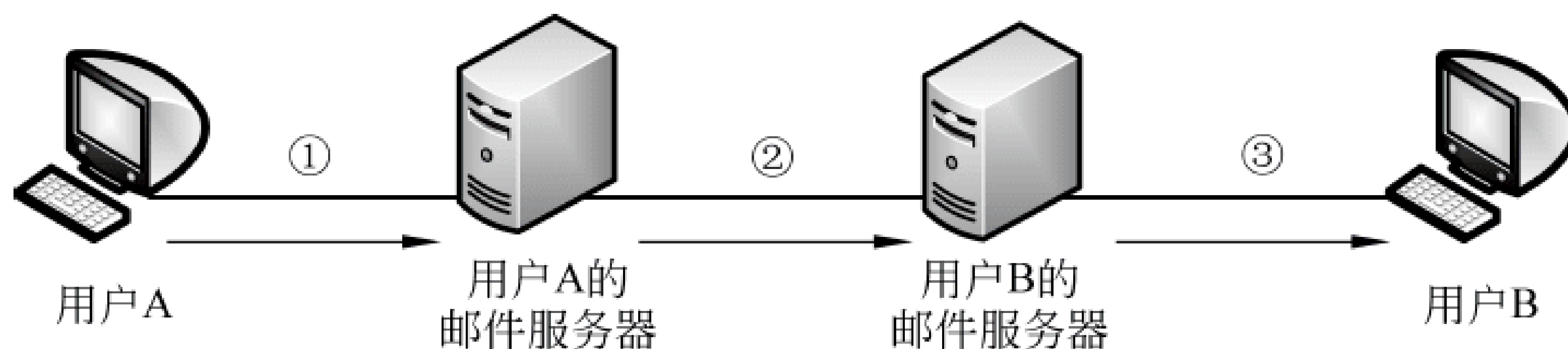


图7-1 用户A与B的邮件系统结构

图中①是用户A与用户A邮件服务器之间的通信协议,应该是SMTP;②是用户A邮件服务器与用户B邮件服务器之间的通信协议,应该也是SMTP协议;③是用户B与用户B的邮件服务器之间的通信协议,即读取邮件的协议按照题目中给出可供选择的协议,只能是POP3协议。

因此,B的描述是正确的。

答案:B。

7-4-5 分析:设计这道习题的目的是帮助读者了解MIME协议的特点。

(1) 最初出现的描述SMTP协议的RFC文档出现在1982年。

(2) SMTP协议的局限性表现在只能发送ASCII码格式的报文,不支持中文、法文、德文,以及语音、视频的邮件的传输。

(3) 通用Internet邮件扩展(MIME)是一种辅助性的协议,它本身不是一个邮件传输协议,只是对SMTP协议的补充。

(4) MIME使用网络虚拟终端(NVT)标准,允许非ASCII码数据通过SMTP传输。

因此,C的描述是错误的。

答案:C。

7-4-6 分析:设计这道习题的目的是帮助读者了解POP3协议的执行过程。

(1) TCP连接建立之后,才能建立POP3会话连接。

(2) 客户在与邮件服务器建立POP3会话连接过程中需要完成身份认证。客户用USER命令向服务器报告用户名,用PASS命令向服务器报告密码。用户名与密码正确,才能进入邮件事务处理阶段。

(3) 在成功完成身份认证之后,POP3会话转入邮件事务处理阶段,客户开始访问POP3邮件服务器。

- 客户向服务器发出STAT请求,了解自己邮箱的状态。
- 服务器返回客户的邮箱长度与邮件数量。
- 客户向服务器发出LIST请求,希望发送邮件列表。
- 服务器返回客户邮箱的邮件列表。
- 客户向服务器发出读邮件的RETR请求。
- 服务器向客户发送邮件。
- 客户向服务器返回正确接收第一个邮件的应答。

• 客户请求删除邮件的 DELE 的请求。

在 POP3 协议中，实际的删除邮件命令是在接收到“退出会话的 QUIT 命令”之后完成。

(4) 当客户希望结束访问邮件服务器时，它将发出 QUIT 退出命令。服务器同意结束会话连接，就发送 Ok 应答报文，并完成有删除标记的邮件。

(5) 客户访问 POP3 服务器的过程结束。

因此，C 的描述是错误的。

答案：C。

7-4-7 分析：设计这道习题的目的是帮助读者了解 IMAP4 协议的主要功能。

IMAP4 是另一种邮件读取协议。Internet 标准 RFC2060 对 IMAP4 进行了定义。IMAP4 提供的功能主要有：

(1) 用户在下载邮件之前可以检查邮件的头部。

(2) 用户在下载邮件之前可以用特定的字符串搜索电子邮件的内容。

(3) 用户可以部分下载电子邮件，这对电子邮件中包含多媒体信息是很有用的。

(4) 用户可以在邮件服务器上创建、删除邮箱，或对邮箱更名，创建分层次的邮箱。

因此，A 的描述是错误的。

答案：A。

7-4-8 分析：设计这道习题的目的是帮助读者了解基于 Web 电子邮件的特点。

(1) 20 世纪 90 年代中期，Hotmail 开发了基于 Web 的电子邮件系统。目前，几乎每个门户网站与大学、公司网站都提供基于 Web 的电子邮件，越来越多的用户使用 Web 浏览器来收发电子邮件。

(2) 在基于 Web 的电子邮件应用中，客户代理就是 Web 浏览器，客户与远程邮箱之间的通信使用的是 HTTP 协议，而不是 POP3 或 IMAP 协议。

(3) 邮件服务器之间的通信仍然使用 SMTP 协议。

因此，C 的描述是错误的。

答案：C。

7.5 Web 与基于 Web 的网络应用

7-5-1 分析：设计该例题的目的是加深读者对主页概念的理解。在讨论主页概念时，需要注意以下几个主要问题：

(1) 在 Web 环境中，信息以 Web 页的形式来显示与链接。Web 页是由 HTML 语言来实现，并在 Web 页之间建立超文本链接以便浏览。

(2) 主页(home page)是指个人或机构的基本 Web 页，用户访问该 Web 网站就会首先看到该网站的主页，通过主页可以访问该网站更进一步的信息。

(3) 主页一般包含文本、图像、表格与超链接信息。

(4) 主页是人们通过 Internet 了解一个学校、公司或政府部门的重要途径。Web 在商业上的重要作用是可以利用主页介绍公司的概况、展示公司新产品的图片、介绍新产品等。

因此，D 关于主页一般包含信息的内容是错误的。

答案：D。

7-5-2 分析：设计这道习题的目的是帮助读者加深对 Web 浏览器工作原理的理解。

答案：当用户在 Web 浏览器中输入域名 www.nankai.edi.cn 访问学校网站时，浏览器可能发送的报文是：

(1) DNS 请求报文——假设浏览器没有访问该网站的记录，它需要通过向关联的 DNS 服务器发出 DNS 请求报文，解析对应该域名的服务器 IP 地址。

(2) ARP 请求报文——根据默认路由器的 IP 地址求解析它的 MAC 地址。

(3) TCP 理解报文——根据 DNS 解析的 Web 服务器 IP 地址，在浏览器与服务器之间建立 TCP 连接。

(4) HTTP 请求报文——向 Web 服务器发送 HTTP 请求报文，获取网中的主页。

(5) ICMP 报文——在 IP 分组传输过程中如果出现各种问题，路由器将与源主机用 ICMP 报文通信。

(6) 源主机需要将各种报文封装在 MAC 帧中传送。

7-5-3 分析：设计该例题的目的是加深读者对 HTTP 无状态协议特点的理解。在讨论 HTTP 协议时，需要注意以下几个主要问题：

(1) HTTP 在传输层使用的是 TCP 协议。

(2) 如果 Web 浏览器想访问一个 Web 服务器，那么 Web 浏览器就需要与 Web 服务器端进程之间建立一个 TCP 连接。一旦 TCP 连接建立之后，用户端的 Web 浏览器进程就可以通过套接字发送 HTTP 请求报文，接收应答报文。

(3) Web 服务器进程通过套接字接收 HTTP 请求报文，发送应答报文。

(4) 由于 TCP 协议提供的是面向连接的可靠服务，Web 浏览器进程发送的 HTTP 请求报文可以正确到达服务器端。同样，Web 服务器进程发送的 HTTP 应答报文也可以正确到达用户端。

(5) 如果报文在传输过程中出现丢失与乱序，也由传输层及一些低层协议去解决，Web 浏览器与 Web 服务器进程不需要干预。

(6) 由于 Web 服务器要面对很多浏览器的并发访问，为了提高 Web 服务器对并发访问的处理能力，因此在设计 HTTP 协议时规定 Web 服务器进程发送的 HTTP 应答报文和文档时，不保存任何发出请求的 Web 浏览器进程状态信息。因此，HTTP 协议属于无状态协议(stateless protocol)。

从以上分析中可以看出，D 关于出错重发处理的描述是错误的。

答案：D。

7-5-4 分析：设计该例题的目的是加深读者对非持续连接 HTTP 协议特点的理解。在讨论 HTTP 协议时，需要注意以下几个主要问题：

(1) HTTP 协议支持非持续连接与持续连接。其中，HTTP/1.0 版协议定义非持续连接，而 HTTP/1.1 默认状态为持续连接。

(2) 如果一个 Web 页包括 1 个基本的 HTLM 文件和 105 个 JPEG 图像文件，那么就称为这个 Web 页是由 106 个对象(object)组成。

(3) 非持续连接中对每次请求/响应都要建立一次 TCP 连接。在非持续连接状态访问该对象的工作过程为：

- HTTP 用户进程在 80 端口发起一次与服务器 www.nankai.edu.cn 的 TCP 连接。

- HTTP 用户进程在这个 TCP 连接上发送一个 HTTP 请求报文，请求报文中包括对象路径 netlab/picture.gif。
- HTTP 服务器在这个 TCP 连接上接收 HTTP 请求报文，从它的存储器中查询出对象 netlab/picture.gif，并封装在一个 HTTP 应答报文，通过这个 TCP 连接发送到用户进程。
- HTTP 服务器进程通知 TCP 协议断开此次 TCP 连接。
- HTTP 用户程序在接收到应答报文之后，通知 TCP 协议断开此次 TCP 连接。同时，用户进程在应答报文中提取 105 个 gif 文件的引用方法。
- HTTP 用户程序对于每个 gif 文件的引用重复一次以上的过程。

（4）在非持续连接工作模式下，用户要读取 105 张图片，必须打开与关闭 106 次 TCP 连接。

从以上分析中可以看出，如果一个 Web 页包括 1 个基本的 HTLM 文件和 100 个 JPEG 图像文件，那么这个 Web 页是由 101 个对象组成。因此，在非持续连接中读取 100 张图片，应该是打开与关闭 101 次 TCP 连接。

答案：D。

7-5-5 分析：设计该例题的目的是加深读者对非持续连接工作模式请求一个 HTTP 文件所需时间的理解。在讨论非持续连接工作模式时，需要注意以下几个主要问题。

（1）当用户从浏览器点击准备浏览一个 Web 文档时，首先要在用户端到服务器端之间"三次握手"建立一个 TCP 连接。假设"三次握手"过程所用时间是从用户端到服务器端再回到用户端的往返时间为 RTT。

（2）第一个往返时间为 RTT 用于用户端到服务器端之间建立一个 TCP 连接。紧接着第二个 RTT 用于用户端向服务器端请求访问 Web 文档的时间之间建立另一个 TCP 连接。服务器端将文档以应答报文的形式发送给用户端的时间为 t_w。那么，请求一个 HTTP 文件所需要的时间 $T \approx 2\text{RTT} + t_w$。

（3）访问图片的 TCP 连接是串行还是并行的，对于请求一个 HTTP 文件所需时间有较大的影响。用户可以通过设置浏览器的相关属性来控制 TCP 连接的并行度。

（4）大部分浏览器允许打开 5～10 个并行的 TCP 连接，每个 TCP 连接处理一个请求/响应事务。并行连接可以缩短用户读取 Web 文档的响应时间。

计算：

（1）采用串行方法获取 85 个 gif 文件所需要的时间

$$T_1 = 2 \times 1500 + (1500 + 3500) \times 85 = 3000 + 425000 = 428000(\text{ms}) = 428(\text{s})$$

（2）采用并行方法（每次连接获取 10 个 gif 文件）获取 85 个 gif 文件所需时间

$$\begin{aligned} T2 &= 2 \times 1500 + [2 \times 1500 + (3500 \times 10)] \times 8 + [2 \times 1500 + (3500 \times 5)] \times 1 \\ &= 3000 + 38000 \times 8 + 20500 \\ &= 3000 + 304000 + 20500 \\ &= 327500(\text{ms}) \\ &\approx 327.5(\text{s}) \end{aligned}$$

答案：

（1）采用串行方法获取 85 个 gif 文件所需时间为 428s。

(2) 采用并行方法(每次连接获取10个gif文件)获取85个gif文件所需时间为327.5s。

7-5-6 分析：设计该例题的目的是加深读者对HTTP持续连接(persistent connection)基本概念的理解。在讨论持续连接概念时，需要注意以下几个主要问题：

(1) HTTP协议支持非持续连接与持续连接。

(2) HTTP/1.0协议支持非持续连接的缺点是：必须为每个请求对象建立和维护一个新的TCP连接。

(3) 在持续连接时，服务器在发出响应后保持该TCP连接，在相同的客户端与服务器端之间的后续报文都通过该连接传送。

(4) 一个包括1个基本的HTLM文件和多个JPEG图形文件的完整Web页可以通过一个持续的TCP连接来传送。

(5) 一个Web服务器中的多个Web页也可以通过一个持续的TCP连接来传送。

(6) Web服务器在接收到客户机的请求或超时才关闭该连接。

从以上分析中可以看出，在持续连接状态中，一个Web服务器中的多个Web页也可以通过一个持续的TCP连接来传送；同时，一个Web服务器中的多个Web页也可以通过一个持续的TCP连接来传送。因此，C的描述是错误的。

答案：C。

7-5-7 分析：设计该例题的目的是加深读者对Web文档类型概念的理解。在讨论Web文档类型时，需要注意以下几个主要问题：

(1) Web文档分为3种类型：静态文档、动态文档与活动文档。

(2) 静态文档的特点：固定内容的文档。它由服务器创建，保存在服务器中。浏览器只能得到文档的副本。

(3) 动态文档的特点：不存在预定义的格式。当浏览器请求到达服务器时，服务器运行创建该文档的应用程序。然后，服务器就将创建的文档作为响应发送给浏览器。由于对每个请求产生一个新的文档，因此每次请求产生的新文档可以是不同的。

(4) 活动文档的特点：需要在浏览器屏幕上产生动画图形，或者需要与用户交互的程序，那么应用程序需要在用户端运行。当用户请求该文档时，服务器就将以二进制代码形式的活动文档发送给浏览器。浏览器收到该活动文档后，存储到存储区中。

从以上分析中可以看出，动态文档的特点是当浏览器提出请求时，服务器运行应用程序创建的文档。因此，C的描述是错误的。

答案：C。

7-5-8 分析：读取整个网站所有网页的时间与网页的数量，以及读一个网页的平均速度有关。

计算：

总的网页数量为1×10^7个；平均读一个网页用100ms；

检索所有网页需要的时间$=(1\times10^7)\times(100\times10^{-3})=1\times10^6$(s)。

检索一个Web网站需要的时间$=(1\times10^6)/(60\times60\times24)=11.6$(天)

答案：检索整个网站最少需要11.6天。

7-5-9 分析：这是一道综合应用题，设计这道习题的目的是帮助读者将MAC层

Ethernet 协议、IP 协议、TCP 协议，以及 Web 协议串联起来思考问题，灵活运用这些知识。

已知条件：

- 网络拓扑。

主机 A 的 MAC 地址是 00-15-C5-C1-5E-28，IP 地址为 10.2.128.100。

- Ethernet 帧前 80B 的十六进制数。

分析：

（1）回答前两个问题需要参考 Ethernet 帧结构与 IP 分组头。图 7-2 是 Ethernet 帧结构示意图。

6B	6B	2B	46~1500B	4B
目的地址	源地址	类型	数据	帧校验字段

图 7-2　Ethernet 帧结构示意图

需要注意的是，通常我们在画 Ethernet 帧结构时，目的地址之前还有 8B 的前导码与帧前定界符。这 8B 在帧接收过程中起作用，接收帧中的有用部分是图 7-2 所示的目的地址、源地址等 5 个字段。Ethernet 帧的前 80B 就是这 5 个字段的部分内容。

Ethernet 帧的前 80B 前 6B 是目的 MAC 地址（01-20-a7-00-51-bb）；之后的 6B 是发送该帧的源 MAC 地址（00-1a-cd-11-50-20）。

题目中已经给出：主机 A 的 IP 地址是 10.2.128.100，MAC 地址是 00-1a-cd-11-50-20。那么，显然主机 A 是发送这个帧的源主机。

（2）将图 7-2 的 Ethernet 帧结构与图 7-3 的 IP 分组头结构结合起来考虑，IP 分组头是放在 Ethernet 帧的数据部分。从源 MAC 地址之后的 2B 进入数据字段，即开始是 IP 分组头。

<table>
<tr><td></td><td></td><td>8</td><td>16</td><td>24</td><td>31</td></tr>
<tr><td>版本</td><td>报头长度</td><td>服务类型</td><td colspan="3">总长度</td></tr>
<tr><td colspan="3">标识</td><td>标志</td><td colspan="2">片偏移</td></tr>
<tr><td colspan="2">生存时间</td><td>协议</td><td colspan="3">头部校验和</td></tr>
<tr><td colspan="6">源IP地址</td></tr>
<tr><td colspan="6">目的IP地址</td></tr>
</table>

图 7-3　IP 分组头结构

IP 分组头的 12B 之后是 4B 的源 IP 地址。那么，可以从图 7-3 看出，IP 分组头中第 13 字节开始是源 IP 地址，再加上帧头的 14（地址 12B＋类型 2B），在表中就是第 27 字节（14＋13＝27）开始是源 IP 地址。那么，源 IP 地址是十六进制数（0a 02 80 64）。我们需要将十六进制转换成二进制，得到源 IP 地址是 10.2.128.100。显然，这与我们前面的分析是一致的，主机 A 是源主机。

主机 A 给 Web 服务器发送请求报文，因此，下一个 4B 目的 IP 地址就是题目中要求的 Web 服务器的 IP 地址。目的 IP 地址值为（40 aa 62 20），将十六进制转换成二进制得

64.170.98.32。那么,Web服务器的IP地址是64.170.98.32。

这里需要注意的一个问题是:Ethernet帧中的目的MAC地址是不是与Web服务器的IP地址对应的MAC地址呢?答案是否定的。Ethernet帧中的目的MAC地址应该是主机A的默认网关地址。

那么,主机A的默认网关地址可以从图7-2的Ethernet帧中找出来,应该是前6B,即:01-20-a7-00-51-bb。

(3)解答第二个问题是考查读者对关于ARP协议的基本概念与工作原理的理解,与题目给出的条件无关。主机A向Web服务器发送请求报文之前,它首先需要用ARP协议去解析目的MAC地址。在构造ARP协议请求包的帧中,目的MAC地址用ff-ff-ff-ff-ff-ff,以广播的方式发送该帧。路由器R2利用NAT功能,将源主机内部地址10.2.128.100转化成请求网络地址192.1.1.15。

(4)根据HTTP/1.1持续的非流水线方式的工作原理,一次请求-响应时间为RTT。这次共需要传输1个Rfc.html网页和5个JPEG小图像,因此从发出请求到收到全部内容,需要经过6个RTT。

(5)IP分组经过路由器R转发时,需要修改IP分组头中的生存时间(TTL)与校验和字段。

答案:

(1)Web服务器的IP地址是64.170.98.32;主机A的默认网关的MAC地址是01-20-a7-00-51-bb。

(2)在构造ARP协议请求包的帧中,目的MAC地址用ff-ff-ff-ff-ff-ff,以广播方式发送该帧。

(3)从发出请求到收到全部内容,需要经过6个RTT。

(4)IP分组经过路由器R转发时,需要修改IP分组头中的生存时间(TTL)与校验和字段。如果IP分组长度超过输出链路的MTU,那么需要修改IP分组头中的总长度、标志、片偏移、生存时间(TTL)与校验和字段。

7.6 即时通信与SIP协议

7-6-1 分析:设计该例题的目的是加深读者对即时通信工作模型的理解。在讨论即时通信工作模型时,需要注意以下几个主要问题:

(1)即时通信工作模型可以分为两种:在线的对等通信方式、离线的中转通信方式。

(2)QQ属于集中式的P2P结构。

(3)QQ用户需要通过在线、手机、电子邮件等申请办法,在QQ服务器上注册并获得自己的用户名与密码。

(4)当用户需要加入QQ网络时,首先在自己计算机上运行QQ用户端软件,然后输入自己的用户名与密码。服务器在验证用户的合法身份后,用户就可以加入QQ网络中。

(5)在登录成功后,QQ用户可以通过服务器下载自己的好友列表、在线信息,以及一些好友发送给他的离线信息。

从以上分析中可以看出,B关于QQ结构的描述是错误的。

答案:B。

7-6-2 分析：设计该例题的目的是加深读者对SIP协议的理解。在讨论SIP协议时，需要注意以下几个主要问题：

(1) SIP是在应用层实现即时通信的控制信令协议。

(2) 在SIP协议中，"会话"是指用户之间的数据传输。传输的数据可以是普通文本数据，可以是音频、视频、E-mail、聊天、游戏等数据。SIP协议用于创建、修改和终止会话。在传输层，SIP可以使用TCP、UDP或流控制传输协议(SCTP)。

(3) SIP协议采用了用户/服务器工作模式，它定义了两种构件与两种状态的代理。这两种构件分别为用户代理(UA)与网络服务器(network server)。

(4) 用户代理包括用户代理客户(UAC)与用户代理服务器(UAS)。用户代理客户发起呼叫，而用户代理服务器则接收呼叫。用户代理客户的表现形式有多种：有些是运行在计算机上的软件，有些是嵌入移动设备(例如笔记本计算机、PDA或移动电话)的软件。

(5) SIP定义了3类网络服务器：代理服务器(proxy server)、注册服务器(registrar)与重定向服务器(redirect server)。

(6) 代理服务器接收用户代理发出的呼叫请求，并将它转发给被叫用户或下一跳的代理服务器，然后由下一跳的代理服务器将呼叫请求转发给代理服务器，因此代理服务器也称为SIP路由器。

(7) 注册服务器接收和处理用户代理请求，完成用户地址注册过程。注册服务器保存用户地址与当前所在位置的映射关系。

(8) 重定向服务器不接收用户呼叫请求，只处理SIP呼叫路由。当它接收到代理服务器呼叫路由请求时，它通过响应报文告诉下一跳代理服务器的地址。代理服务器根据该地址重新向下一跳的代理服务器发送呼叫请求报文。

(9) SIP协议使用的地址可以是电话号码，也可以是电子邮件地址或IPv4地址。SIP协议要求的地址格式可以为：

- 电话号码　　sip:wugongyi@8622-23508917
- IPv4地址　　sip:wugongyi@202.1.2.180
- 电子邮件地址　　sip:wugongyi@nankai.edu.cn

从以上分析中可以看出，A关于SIP属于传输层协议的描述是错误的。

答案：A。

7-6-3 分析：设计该例题的目的是加深读者对SIP协议C/S工作模式的理解。

在讨论SIP协议时，需要注意以下几个主要问题：

(1) SIP协议采用了客户/服务器工作模式，它定义了两种构件与两种状态的代理。这两种构件分别为用户代理(User Agent，UA)与网络服务器(network server)。

(2) 用户代理包括两个程序：用户代理客户(User Agent Client，UAC)与用户代理服务器(User Agent Server，UAS)。

(3) 用户代理客户发起呼叫，而用户代理服务器则接收呼叫。

(4) 用户代理客户的表现形式有多种，有些是运行在计算机上的软件，有些是嵌入到移动设备(例如笔记本计算机、PDA或移动电话)的软件。

因此，D的描述是错误的。

答案：D。

7-6-4 分析：设计该例题的目的是加深读者对 SIP 网络服务器特点的理解。

在讨论 SIP 网络服务器特点时，需要注意以下几个主要问题：

(1) SIP 定义了 3 类网络服务器：代理服务器(proxy server)、注册服务器(registrar)与重定向服务器(redirect server)。

(2) 代理服务器接收用户代理客户发出的呼叫请求，并将它转发给被叫用户或下一跳的代理服务器，然后由下一跳的代理服务器将呼叫请求转发给用户代理服务器，因此代理服务器也称为“SIP 路由器”。

(3) 注册服务器接收和处理用户代理请求，完成用户地址注册过程。注册服务器保存用户地址与当前所在位置的映射关系。

(4) 重定向服务器不接受用户呼叫请求，只处理 SIP 呼叫路由。当它接收到代理服务器呼叫路由请求时，它通过响应报文告诉下一跳代理服务器的地址。代理服务器根据该地址重新向下一跳的代理服务器发送呼叫请求报文。

(5) SIP 定义了代理服务器的两种状态：有状态代理与无状态代理。其中，有状态代理服务器保存接收到的用户代理接入请求、回送的响应，以及转发的请求信息。无状态代理服务器在转发请求信息之后不保留状态信息。

因此，A 的描述是错误的。

答案：A。

7.7 主机配置与动态主机配置协议 DHCP

7-7-1 分析：设计该例题的目的是加深读者对主机配置与 DHCP 协议的理解。在讨论主机配置与 DHCP 协议时，需要注意以下几个主要问题：

(1) 对于 TCP/IP 网络来说，要将一台主机接入 Internet 中必须配置的参数主要有：本地网络的默认路由器地址、网络掩码、为主机提供服务的服务器地址、IP 分组的生存时间 TTL 值等。

(2) 对于远程主机、移动设备、无盘工作站和地址共享的配置，手工方法是不可能完成的。

(3) RARP 是第一个在网络层解决无盘工作站引导问题的协议。RARP 的优点是简单和易于实现；缺点是不适用不同类型的局域网，不支持对主机的配置。代替 RARP 协议的是引导协议 BOOTP。

(4) BOOTP 缺少对动态 IP 地址分配的支持，而 20 世纪 90 年代对动态 IP 地址分配的需求变得十分迫切，这种需求导致了动态主机配置协议(DHCP)的出现。DHCP 是在 BOOTP 基础上发展起来的，并且设计者 BOOTP 协议与 DHCP 协议都放在应用层。

(5) DHCP 可以为主机自动分配 IP 地址及其他一些重要参数。将 DHCP 协议放在应用层的理由是：协议操作不依赖于低层的硬件；在网络之间传送主机配置文件，这点是网络层协议无法实现的。

(6) DHCP 提供一种“即插即用联网”机制，它允许一台主机接入网络之后就可以自动获取一个 IP 地址与相关参数。同时，DHCP 协议可以为各种服务器分配一个永久的 IP 地址。在服务器重新启动时，IP 地址不变。

从以上分析中可以看出，C 的描述是错误的。

答案：C。

7-7-2 分析：设计这道习题的目的是帮助读者了解 DHCP 服务器的功能。

DHCP 协议是基于客户/服务器工作模式。DHCP 服务器是一个为客户计算机提供动态主机配置服务的网络设备。DHCP 服务器的功能主要是：

(1) 地址储存与管理。

DHCP 服务器储存 IP 地址，记录哪些 IP 地址已经被使用，哪些 IP 地址仍然可用。

(2) 配置参数的存储和管理。

DHCP 服务器储存和维护其他的主机配置参数。

(3) 租用管理。

DHCP 服务器用租用的方式将 IP 地址动态地分配给主机，并管理 IP 地址的租用期(lease period)。DHCP 服务器维护批准租用给主机的 IP 地址信息，以及租用期长度。RFC1533 规定租用期用 4 字节的二进制数来表示，单位为秒。

(4) 响应客户主机请求。

DHCP 服务器响应主机发送的请求分配地址、传送配置参数，以及租用的批准、更新与终止等各种类型的请求。

(5) 服务管理。

DHCP 服务器允许管理员查看、改变和分析有关地址、租用、参数等，以及与 DHCP 服务器运行相关的信息。

因此，B 的描述是错误的。

答案：B。

7-7-3 分析：设计这道习题的目的是帮助读者了解 DHCP 客户端的功能。

DHCP 客户机的功能主要是：

(1) 发起配置。

DHCP 客户机可以随时向 DHCP 服务器发起获取 IP 地址与配置参数的协商过程。

(2) 配置参数管理。

DHCP 客户机可以从 DHCP 服务器获取全部或部分配置参数，并维护配置参数。

(3) 租用管理。

DHCP 客户机可以更新租用期，在无法更新时进行重绑定，在不需要时提前终止租用。

(4) 报文重传。

DHCP 协议采用不可靠的 UDP 协议，DHCP 客户机要负责检测 UDP 报文是否丢失，以及丢失之后的重传。

因此，D 的描述是错误的。

答案：D。

7-7-4 分析：设计这道习题的目的是帮助读者进一步掌握 DHCP 客户端与服务器交互过程。

DHCP 客户端与服务器的交互过程为：

(1) DHCP 客户端需要安装 DHCP 协议构造一个 IP 租用请求 DHCPDISCOVER 报文，以广播方式发送出去，客户进入初始化状态。

(2) 凡是接收到 DHCP 客户端请求报文的 DHCP 服务器都要返回一个 DHCPOFFER

应答报文。DHCPOFFER 应答报文中包括有分配给 DHCP 客户端的 IP 地址、租用期及其他参数。

(3) 可能收到多个 DHCPOFFER 应答报文的 DHCP 客户端,从中选择一个 DHCP 服务器;然后向被选择的 DHCP 服务器发送一个 DHCPREQUST 请求报文,作为对它所选服务的回应。

(4) 被选择的 DHCP 服务器向 DHCP 客户端发送一个 DHCPACK 应答报文。当 DHCP 客户端接收到 DHCPACK 应答报文之后,客户端才可以使用分配的临时 IP 地址,进入"已绑定状态"。

在初始阶段,DHCP 客户端以广播方式发送一个 IP 租用请求 DHCPDISCOVER 报文。因此,A 的描述是错误的。

答案:A。

7-7-5 分析:设计这道习题的目的是帮助读者进一步掌握 DHCP 租用信息的具体内容。

DHCP 服务器通过租用方式将 IP 地址动态分配给主机,并管理 IP 地址的租用期(lease period)。DHCP 服务器维护批准租用给主机的 IP 地址信息,以及租用期长度。RFC1533 规定租用期用 4 字节的二进制数来表示,单位为秒。

因此,D 的描述是错误的。

答案:D。

7-7-6 分析:

解决这类问题的基本方法是读懂题目中图表所提供的信息。

(1) 题目图中①对应的是用户发出 DHCP 请求报文使用的源 IP 地址是 0.0.0.0。

(2) 题目图中②对应的是广播地址 255.255.255.255。

(3) 题目图中③对应的是用户发出报文类型是 DHCP discover。

(4) 题目图中④对应的广播地址 255.255.255.255。

(5) 题目图中⑤对应的是 DHCP ack。

答案:

① 0.0.0.0

② 255.255.255.255

③ DHCP discover

④ 255.255.255.255

⑤ DHCP ack

7-7-7 分析:

解决这类问题的基本方法是读懂题目中图解析的报文交互过程,并从中获取有用的信息。

(1) 用户从 DHCP 获得的 IP 地址是 Client address=211.80.20.120;
用户的 MAC 地址 Client hardware address=05F12245F6。

(2) DNS 服务器的 IP 地址 Domain Name Server address=211.25.110.8;
路由器的 IP 地址 Gateway address=211.80.20.2。

(3) DHCP 服务器的 IP 地址可从报文的源地址找出为 211.80.20.1。

答案：

（1）用户从 DHCP 获得的 IP 地址是 211.80.20.120；
用户的 MAC 地址是 05F12245F6。

（2）DNS 服务器的 IP 地址是 211.25.110.8；
路由器的 IP 地址是 211.80.20.2。

（3）DHCP 服务器的 IP 地址是 211.80.20.1。

7.8 网络管理与 SNMP 协议

7-8-1 分析：设计该例题的目的是加深读者对网络管理概念的理解。在讨论网络管理概念时，需要注意以下几个主要问题：

（1）网络管理的目的是：使网络资源能得到有效利用，网络出现故障时能及时报告和处理，以保证网络能够正常、高效地运行。

（2）网络管理系统通常由 5 个部分组成：管理进程（manager）、被管对象（managed object）、代理进程（agent）、管理信息库（MIB）和网络管理协议。

（3）管理进程是网络管理的主动实体，它提供网络管理员与被管对象之间的界面，完成网络管理员指定的各项管理任务，读取或改变被管对象的网络管理信息。

（4）被管对象指网络上的软硬件设备，例如交换机、路由器、主机与服务器等。

（5）代理进程执行管理进程（例如系统配置、数据查询）的命令，向管理进程报告本地出现的异常情况。

（6）在 SNMP 网络管理模型中，代理可以分为两种类型：管理代理与外部代理。

- 管理代理是在被管理的设备中加入的执行 SNMP 协议的程序。
- 外部代理（proxy agent）是指在被管设备外部增加的执行 SNMP 协议的程序或设备。

（7）网络管理协议规定了管理进程与代理进程之间交互的网络管理信息的格式、意义与过程。目前流行的网络管理协议主要有：TCP/IP 协议体系的简单网络管理协议（SNMP）与 OSI 参考模型的公共管理信息协议（CMIP）。

（8）管理信息库是一个概念上的数据库。被管对象信息存放在管理信息库（MIB）中。

- 代理进程可以读取和修改本地 MIB 中的各种变量值。
- 每个代理进程管理自己的本地 MIB，并与管理进程交换网络状态信息。
- 多个本地 MIB 共同构成整个网络的 MIB。

从以上分析中可以看出，B 关于网络管理系统组成的描述是错误的。

答案：B。

7-8-2 分析：设计该例题的目的是加深读者对 SNMP 协议的理解。在讨论 SNMP 协议时，需要注意以下几个主要问题：

（1）SNMP 应该包括两部分内容：SNMP 体系结构与 SNMP 协议。SNMP 体系结构通常由 5 部分组成：管理进程（manager）、被管对象、代理进程（agent）、管理信息库（MIB）、网络管理协议 SNMP 等。

（2）当一个网络资源不能与管理进程直接交换管理信息时，就需要使用外部代理。例如，集线器、调制解调器、简单的交换机，以及有些便携式设备 PDA，它们不支持复杂的网络管理协议。这时，就需要为这类网络设备增加外部代理。外部代理按照 SNMP 协议与网络

管理进程通信,还要与被管理的网络设备通信。一个外部代理应该能够管理多个网络设备。

(3) 网络管理受到网络拓扑、网络规模、网络设备类型、网络状态的动态变化等因素的影响。从 SNMP 协议的基本内容上,SNMP 协议的交互过程简单,只规定 5 种消息对网络进行管理。为了简化和降低通信代价,它在传输层采用简单的 UDP 协议。

从以上分析中可以看出,D 关于 SNMP 在传输层采用协议的描述是错误的。

答案:D。

7-8-3 分析:设计该例题的目的是加深读者对 SNMP 基本操作的理解。在讨论 SNMP 的基本操作时,需要注意以下几个主要问题:

(1) SNMP 采用轮询方式,周期性通过“读”、“写”两种操作来实现基本的网络管理功能。

(2) 网络管理进程通过向代理进程发送 Get 报文检测被管对象状态,使用 Set 报文来改变被管对象状态。

(3) 除了轮询方式之外,网络管理进程也允许被管对象在重要事件发生时,使用 Trap 报文向网络管理进程报告。

从以上分析中可以看出,C 关于 Set 报文的描述是错误的。

答案:C。

7-8-4 分析:设计该例题的目的是加深读者对 SNMP 协议被管对象命名方法的理解。

在讨论 SNMP 协议被管对象的命名方法时,需要注意以下几个主要问题:

(1) SMI 规定标识所有被管对象的对象命名树(object naming tree)方法。对象命名树没有根,节点标识符用小写英文字母表示。

(2) 对象命名树的结构的顶级有 3 个对象:ITU-T 标准、ISO 标准,以及两者联合的标准。

① ITU-T 的前身是 CCITT,它们都是世界上最主要的标准制定组织,在对象命名树中标识符的标号分别为 0、1、2。

② ISO 之下也有多个对象,其中标号为 3 的是为其他国际组织建立的子树,称为 org。

③ 在 org 之下有一个美国国防部 dod 的子树,标号为 6。

④ 在 dod 之下有一个 Internet 的子树,标号为 1。如果只讨论 Internet 之下的子树,那么只需在对象标识符旁标出 iso. org. dod. internet,或标号 1. 3. 6. 1。

⑤ 在 internet 节点之下,标号 2 的节点是网络管理 mgmt,表示为 iso. org. dod. internet. mgmt,或标号 1. 3. 6. 1. 2;标号为 4 的节点 private 是供私有公司使用的,表示为 iso. org. dod. internet. private,或标号 1. 3. 6. 1. 4。

⑥ 在 mgmt 节点之下,只有一个节点管理信息库 mib-2,其对象标识符标号为 iso. org. dod. internet. mgmt. mib-2 或标号 1. 3. 6. 1. 2. 1。在 private 之下,有一个 enterprise 的子树,其对象标识符标号为 iso. org. dod. internet. private. enterprise 或标号 1. 3. 6. 1. 4. 1。

⑦ 在 enterprise 的子树中,标号为 9 的是分配给 Cisco 公司的。所有 Cisco MIB 对象都是从 1. 3. 6. 1. 4. 1. 9 开始。

(3) MIB 对象的定位。

所有 MIB 对象都以对象命名树中的两个分支来命名:

① 常规 MIB 对象。

常规 MIB 对象不是由某个厂商规定,而是按照 SNMP 标准规定,这些对象都在 mgmt(2)节点之下的 mib-2(1)子树(1. 3. 6. 1. 2. 1)中。

② 专用MIB对象。

由硬件制造商创建的、用于某个网络管理系统制造商的专用对象位于private(4)之下的enterprise(1)子树(1.3.6.1.4.1)中。

假设公司在enterprise的子树之下有一个MIB节点号150,它是为新款服务器产品申请的产品标识符编号为50,那么服务器对象标识符应该为1.3.6.1.4.150.50。

答案:1.3.6.1.4.150.50。

7.9 典型应用层协议——FTP的分析

7-9-1 分析:设计该例题的目的是加深读者对FTP用户程序特点的理解。在讨论FTP用户程序时,需要注意以下几个主要问题:

(1) 常用的FTP用户程序有3种类型:传统的FTP命令行、浏览器与FTP下载工具。

(2) 传统的FTP命令行是最早的FTP用户程序。

(3) 浏览器软件支持访问FTP服务器,可以直接登录到FTP服务器并下载文件。

(4) 在使用FTP命令行从FTP服务器下载文件时,如果在下载过程中网络连接意外中断,已经下载完的那部分文件将会前功尽弃。

(5) FTP下载工具就可以解决这个问题,通过断点续传功能就可以继续传输剩余部分。目前,常用的FTP下载工具主要有:CuteFTP、LeapFTP、AceFTP、BulletFTP与WS FTP等。

从以上分析中可以看出,C关于断点续传功能的描述是错误的。

答案:C。

7-9-2 分析:设计该例题的目的是加深读者对FTP协议工作模型的理解。在讨论FTP协议工作模型时,需要注意以下几个主要问题:

(1) FTP工作模型的一个重要特点是:使用控制连接、数据连接两个并行的TCP连接来完成文件传输。

(2) 用于控制连接的FTP服务器端使用的熟知端口号为21。

(3) 用于数据连接的FTP服务器端使用的熟知端口号为20。

(4) FTP客户端包括3部分:用户接口、控制进程、数据进程。

(5) FTP服务器端包括2部分:控制进程、数据进程。

从以上分析中可以看出,C关于用于控制连接的FTP客户端使用临时端口号的描述是错误的。

答案:C。

第三部分　综合练习——术语解析

从给出的26个定义中挑出20个,并将标识定义的字母填在对应术语前的空格位置。

(1)________覆盖网　　(2)________应用层协议

(3)________外部代理　　(4)________配置管理

(5)________域名解析　　(6)________权威域名服务器

(7)________无状态协议　　(8)________根域名服务器

(9)________ DHCP　　　　(10)________ HTML

(11)________ URL　　　　(12)________搜索引擎

(13)________租用期　　　　(14)________对象命名树

(15)________ MIB　　　　(16)________ SIP

(17)________ NVT　　　　(18)________本地域名服务器

(19)________ DNS　　　　(20)________应用程序体系结构

A. 规定了应用程序进程之间通信所遵循的通信规则。

B. 实现电子邮件服务服务功能的协议。

C. 实现交互式文件传输服务服务功能的协议。

D. 实现人们对所关心的问题开展专题讨论服务功能的协议。

E. 实现终端远程登录服务功能的协议。

F. 在 IP 网络上构建的一种逻辑的覆盖网。

G. 支持 Internet 运行的全局基础设施类应用层协议。

H. 支持各个网络系统运行的局部基础设施类应用层协议。

I. 对于 DNS 系统的整体运行具有极重要作用的最高级别服务器。

J. 每个"区"用来保存该区内所有主机域名与 IP 地址映射关系数据的服务器。

K. 将域名转换为对应的 IP 地址的过程。

L. TELNET 用户进程与服务器进程之间的通信协议。

M. 邮件用户端向邮件服务器发送邮件时使用的协议。

N. Web 系统中对资源的位置和访问方法的标识。

O. 运行在 Web 上对信息进行理解、提取、组织和处理的应用软件。

P. 可以使用 sip:wugongyi@8622-23508917 地址的协议。

Q. DHCP 服务器管理的用户 IP 地址使用时间。

R. SNMP 标识所有被管对象的方法。

S. SNMP 被管对象的信息都存放在的位置。

T. SNMP 配置管理监控网络拓扑、设备与链路互连情况的功能。

U. 在被管设备外部增加的执行 SNMP 协议的程序或设备。

V. 每个 ISP、一所大学,甚至是一个系都可能有的域名服务器。

W. 创建网页所用的语言。

X. 包含个人或机构基本信息的页面。

Y. HTTP 协议的一个基本属性。

Z. 网络应用程序功能、工作模型与协议结构。

参考答案

(1) F	(2) A	(3) U	(4) T	(5) K
(6) J	(7) Y	(8) I	(9) H	(10) W
(11) N	(12) O	(13) Q	(14) R	(15) S
(16) P	(17) L	(18) V	(19) G	(20) Z

第 8 章 网络安全

第一部分 同步练习

8.1 网络安全基本概念

8-1-1 以下关于网络安全特点的描述中，错误的是________。

A. 网络安全是一个系统的社会工程

B. 网络安全已经危及国家网络空间安全

C. 网络安全涉及技术、政策、道德与法律法规

D. 网络协议 TCP/IP 的安全性有效地降低了网络攻击的成功性

8-1-2 以下关于网络安全威胁发展趋势的描述中，错误的是________。

A. 趋利性是当前网络攻击的主要特点

B. 网络攻击开始演变成某些国家或利益集团重要的政治、军事工具

C. 网络攻击、僵尸网络与特洛伊木马已成为网络安全的三大公害

D. 网络攻击向无线与 P2P 网络扩张

8-1-3 以下关于信息传输中攻击类型的描述中，错误的是________。

A. 目的节点没有收到信息，信息在传输中被攻击者非法截获，造成信息泄露

B. 目的节点接收到信息，都是信息在传输中被攻击者非法窃听

C. 攻击者将截获的信息进行修改或插入欺骗性的信息，然后发送给目的节点

D. 攻击者冒充源节点将伪造的信息发送给目的节点

8-1-4 以下关于非服务攻击特点的描述中，错误的是________。

A. 非服务攻击不可能攻击到通信线路

B. 攻击者可能使用各种方法对路由器进行攻击

C. 攻击使得网络通信设备出现严重阻塞甚至瘫痪

D. 局域网交换机属于数据链路层设备，不在非服务攻击的范畴

8-1-5 以下关于漏洞攻击的描述中，错误的是________。

A. 漏洞攻击是网络攻击者利用网络中存在的漏洞，非法访问网络、窃取信息的现象

B. 漏洞是指软件、协议的漏洞

C. 攻击之前要通过踩点、扫描、拓扑探测、信息流监视等多种形式寻找出漏洞

D. ping、traceroute、tcpdump 等常规网络管理与测试软件都可能成为漏洞扫描工具

8-1-6 以下关于欺骗攻击的描述中,错误的是________。

A. 利用破解口令与 IP 欺骗等方法,达到非法访问目的的攻击属于欺骗攻击

B. 入侵者采用穷举法或口令猜测程序,破译用户账号和密码

C. 重放攻击属于一种 IP 欺骗攻击

D. 蜜罐属于欺骗攻击

8-1-7 以下关于僵尸网络特征的描述中,错误的是________。

A. 被攻击主机上有大量等待的 TCP 连接

B. 大型的 botnet 网络最多可能绑架数千个攻击执行器

C. 大量无用数据包造成网络拥塞,使被攻击的主机无法正常地与外界通信

D. 被攻击主机无法正常回复合法用户的服务请求,严重时会造成主机系统瘫痪

8-1-8 以下描述中不属于网络安全服务基本功能的是________。

A. 数据保密　　B. 数据完整　　C. 防抵赖　　D. 数字签名

8.2 加密与认证技术

8-2-1 以下关于密钥概念的描述中,错误的是________。

A. 密码体制的两个基本构成要素是加密/解密算法和密钥

B. 密钥为常量,加密算法为变量

C. 加密算法和解密算法的操作通常都是在一组密钥控制下进行

D. 对于同一种加密算法,密钥的位数越长,安全性也就越好

8-2-2 以下关于对称密码体系的描述中,错误的是________。

A. 对称加密技术存在着通信双方之间确保密钥安全交换的问题

B. 如果一个用户要与 N 个其他用户进行加密通信时需要有 N^2 个密钥

C. 密钥在加密方和解密方之间的传递和分发必须通过安全通道进行

D. 密钥管理涉及密钥的产生、分配、存储、销毁

8-2-3 以下关于非对称密钥密码体系的描述中,错误的是________。

A. 非对称密钥密码体制中的加密公钥可以公开

B. 理论上要保证从公钥和密文中分析出私钥在计算上是不可行的

C. 如果用公钥作为加密密钥,私钥作为解密密钥,则可以数字签名

D. 网络中 N 个用户之间进行通信加密仅需要使用 N 对密钥

8-2-4 以下关于公钥基础设施 PKI 的描述中,错误的是________。

A. PKI 是基于对称加密密码体系

B. PKI 系统的工作对用户是透明的

C. PKI 主要任务是确定用户可信任的数字身份

D. PKI 建立在安全通信信任平台与密钥管理体系之上

8-2-5 以下关于 PKI 工作原理的描述中,错误的是________。

A. 认证中心 CA 产生用户之间通信时使用的非对称加密的公钥与私钥对

B. 注册认证 RA 中心确认申请下载数字签名密钥用户的合法身份

C. 接收文件的用户用公钥验证文件的合法性

D. PKI 系统中只能有一个 CA 中心

8-2-6 以下关于数字签名基本概念的描述中,错误的是________。

A. 亲笔签名是用来保证文件或资料真实性的一种方法

B. 接收方可以核对发送方对报文的签名,以确定对方的身份

C. 目前广泛应用的数字签名算法是非对称密钥体系的消息摘要 MD5 算法

D. 发送方用 MD5 算法对文件数据进行加密运算

8.3 网络安全协议

8-3-1 以下关于 IPSec 主要特征的描述中,错误的是________。

A. IPSec 的安全服务工作在网络层

B. IPSec 是由多种安全协议与加密算法构成的一个安全体系

C. IPSec 定义了两种保护 IP 分组的模式:传输模式与隧道模式

D. IPSec 对于 IPv4 与是 IPv6 可选的

8-3-2 以下关于 SSL 协议基本概念的描述中,错误的是________。

A. SSL 协议为 Web 客户与服务器之间的用户身份认证与安全数据传输提供服务

B. SSL 协议工作在传输层

C. 当 Web 系统采用 SSL 协议时,Web 客户端使用 https

D. OpenSSL 软件包支持 SSLv3 与 TLSv1 版本

8-3-3 以下关于 SET 协议特点的描述中,错误的是________。

A. SET 协议已成为目前公认的最成熟的应用层电子支付安全协议

B. SET 协议采用数字信封技术保护交易中数据交换的秘密性

C. SET 协议通过信用卡实现对通信实体之间、持卡人身份、商家身份的身份认证

D. SET 协议通过数字签名保证系统内部交换信息在传输过程中不被篡改与伪造

8.4 防火墙技术

8-4-1 以下关于防火墙功能的描述中,错误的是________。

A. 检查所有从外部网络进入内部网络的数据包

B. 检查所有从内部网络流出到外部网络的数据包

C. 对于不同协议的分组进行格式变换

D. 具有防攻击能力,保证自身的安全性的能力

8-4-2 以下关于防火墙系统结构的描述中,错误的是________。

A. 构成防火墙系统的两个基本部件是包过滤路由器和应用级网关

B. 包过滤路由器按照分组过滤规则,只需要根据 IP 地址决定该分组是否应该转发

C. 最简单的防火墙由一个包过滤路由器组成

D. 复杂的防火墙系统是由包过滤路由器和应用级网关多种组合方式

8.5 入侵检测技术

8-5-1 以下关于入侵检测基本概念的描述中,错误的是________。

A. IDS 是用于识别计算机和网络资源恶意使用行为的系统

B. IDS监测和发现可能存在的攻击行为,采取相应的防护手段

C. IDS检查系统的配置和漏洞

D. IDS对用户口令进行加密与解密

8-5-2 以下关于入侵检测系统结构的描述中,错误的是________。

A. IDS一般由事件、事件发生器、事件分析器、响应单元组成

B. IDS需要分析的数据统称为事件

C. 事件分析器根据入侵特征描述、行为模型来判断事件的性质

D. 响应单元根据分析结果做出切断连接、改变文件属性或报警等响应

8-5-3 以下关于入侵检测方法的描述中,错误的是________。

A. 误用检测系统的主要问题是确定攻击特征模式可以覆盖实际攻击的所有要素

B. 入侵检测方法可以分为异常检测、误用检测,以及两种方法结合

C. 异常检测系统的关键是建立一个对应正常网络活动的特征原型

D. 所有异常活动都是入侵活动

8-5-4 以下关于IDS分类的描述中,错误的是________。

A. IDS可以分为基于主机、基于网络与分布式IDS

B. 基于主机的IDS一般以计算机的系统日志、应用程序日志为数据源

C. 基于网络的IDS能主动发现网络入侵事件

D. 分布式IDS不仅检测针对单机的入侵,也能检测针对整个网络主机的入侵

8.6 网络业务持续性规划技术

8-6-1 以下关于网络文件备份基本方法的描述中,错误的是________。

A. 选择备份设备应根据网络文件系统的规模、文件的重要性来决定

B. 选择备份程序应注意备份程序支持哪种网络操作系统与设备等因素

C. 建立备份制度计划表的第一件事是选择需要备份的文件和备份的时间

D. 任何一种备份方法都能保证恢复系统时数据不丢失

8-6-2 以下关于业务可持续性规划技术的描述中,错误的是________。

A. 业务持续性规划是针对各种可能发生的突发事件提前制定预案

B. 业务持续性规划的第一步是风险分析

C. 业务持续性规划的主要任务是如何缩短对数据访问的恢复时间

D. 数据恢复规划涉及远程镜像与数据恢复方法

8.7 网络防病毒技术

8-7-1 以下关于特洛伊木马特点的描述中,错误的是________。

A. 一种嵌入到一些正常软件中的恶意软件

B. 专为欺骗用户,让用户以为它是友好程序而设计

C. 不改变或感染其他的文件,只是伪装成一种正常程序

D. 从一台被感染的主机通过自复制传染给其他机器

8-7-2 以下关于垃圾邮件定义的描述中,错误的是________。

A. 收件人无法拒收的电子邮件

B. 广告、电子刊物、各种形式的宣传品等宣传性的电子邮件
C. 含有虚假的信息源、发件人、路由等信息的电子邮件
D. 隐藏发件人身份、地址、标题等信息的电子邮件

第二部分　同步练习答案与解析

8.1　网络安全基本概念

8-1-1　分析：设计这个例题的目的是加深读者对于网络安全特点的理解。理解网络安全的特点，需要注意以下几个基本问题：

(1) 网络安全研究一直伴随着网络技术与应用的发展而进步。

(2) 网络安全问题实际上是个社会问题，仅靠技术来解决这些问题是不可能的。

(3) 网络安全危及国家空间安全，已经成为危及国家安全与稳定的大问题。

(4) 每个国家只能立足于本国，研究网络安全技术，培养专门人才，发展网络安全产业，才能构筑本国的网络与信息安全防范体系。

因此，D 关于网络安全与 TCP/IP 协议关系的描述是错误的。

答案：D。

8-1-2　分析：设计这个例题的目的是加深读者对于网络安全威胁发展趋势的理解。理解网络安全威胁发展趋势，需要注意以下几个基本问题：

(1) 趋利性是当前网络攻击的主要特点。受经济利益驱动，网络攻击的动机已经从初期的恶作剧、显示能力、寻求刺激，攻垮路由器、黑网站等明显的破坏性攻击，转向利用漏洞攻击的方法，绕过网络防护系统，悄悄窃取有价值的用户信息(如用户名、密码、银行与网上交付信息、QQ 号等)，并逐步向有组织犯罪，甚至是有组织的跨国经济犯罪发展。

(2) 网络攻击开始演变成某些国家或利益集团重要的政治、军事工具。多个发达国家组建网络站司令部、网络部队的举动就明显地表明，网络安全已经上升到国家安全战略的地位；同时也表明，网络攻击开始演变成某些国家或利益集团的重要的政治、军事工具，甚至是恐怖分子活动的工具。

(3) 网络攻击、病毒与垃圾邮件是网络安全的三大公害。网络攻击、病毒与垃圾邮件攻击方式相互融合，变种不断出现。利用垃圾邮件传播病毒，利用病毒实施网络攻击的态势已经明朗。同时，利用漏洞制造病毒的速度加快，病毒已经从传统的 Internet 向无线与 P2P 网络扩张，网络病毒的危害继续呈上升的趋势。

(4) 物联网、云计算与三网融合面临着更为严峻的网络安全问题。新的网络应用技术不断出现，使得网络攻击的类型不断演变。针对三网融合多传输平台的网络攻击形式正在发生变化。无线网络与移动 Internet 应用已经成为网络攻击新的重点目标。物联网面临着更为严峻的网络安全威胁问题。利用 Web 直接攻击云计算平台的形式已经出现，可信的安全云计算、个人隐私保护研究已经成为目前信息安全研究的热点问题。

因此，C 关于网络安全三大公害的描述是错误的。

答案：C。

8-1-3　分析：设计这个例题的目的是加深读者对于信息传输过程中可能存在攻击类型的理解。理解网络安全威胁发展趋势，需要注意以下几个基本问题：

(1) 截获信息是信息从源节点传输出来,中途被攻击者非法截获,目的节点没有接收到应该接收的信息,造成信息在传输途中丢失。

(2) 窃听信息是信息从源节点传输到目的节点,但中途被攻击者非法窃听。尽管目的节点接收到信息,信息并没有丢失,如果被窃听到的是重要的政治、军事、经济信息,那么也有可能造成严重的问题。

(3) 篡改信息是指信息从源节点传输到目的节点的中途被攻击者非法截获,攻击者将截获的信息进行修改或插入欺骗性的信息,然后将篡改后的错误信息发送给目的节点。尽管目的节点也会接收到信息,好像信息没有丢失,但是接收的信息却是错误的。

(4) 伪造信息是源节点并没有信息要传送到目的节点。攻击者冒充源节点将伪造的信息发送给了目的节点。目的节点接收到的是伪造的信息。如果目的节点没有办法发现信息是伪造的,那么就可能出现严重的问题。

因此,A 关于截获信息特点的描述是错误的。

答案:A。

8-1-4 分析:设计这个例题的目的是加深读者对于非服务攻击的特点的理解。理解非服务攻击的特点,需要注意以下几个基本问题:

(1) Internet 中的网络防攻击可以归纳为以下两种基本类型:服务攻击与非服务攻击。

(2) 服务攻击是指攻击者对 E-mail、FTP、Web 或 DNS 服务器发起攻击,造成服务器工作不正常,甚至造成服务器瘫痪。

(3) 非服务攻击不针对某项具体应用服务,而是针对网络设备或通信线路。攻击者可能使用各种方法对网络通信设备(例如路由器、交换机、防火墙、网关)与通信线路发起攻击,使得网络通信设备出现严重阻塞甚至瘫痪,或者是造成线路阻塞,最终使网络通信中断。

因此,D 关于交换机与非服务攻击关系的描述是错误的。

答案:D。

8-1-5 分析:设计这个例题的目的是加深读者对于漏洞攻击特点的理解。理解漏洞攻击的特点,需要注意以下几个基本问题:

(1) 网络攻击的趋利性使得我们越来越重视网络漏洞攻击的研究。

(2) 漏洞攻击是指:网络攻击者通过网络踩点、漏洞扫描、网络拓扑探测、信息流监视等多种形式,利用网络中存在的漏洞,非法访问网络、窃取信息的现象。

(3) 漏洞可以分为两类:技术漏洞与管理漏洞。

(4) 技术漏洞主要是指:网络协议设计时存在的瑕疵、协议软件与应用软件的瑕疵,以及系统和网络的配置错误。

(5) 管理漏洞包括网络使用与管理权限、密码保护措施的不足。无论技术或者管理的漏洞都为攻击者提供了可乘之机。

(6) 黑客通过网络踩点来发现目标主机或网络;利用各种漏洞扫描工具,如 ping、traceroute、tcpdump 等常规网络管理与测试软件与专用的黑客工具,或通过信息流监视的方法,以及来搜集和发现操作系统、网络拓扑、路由器与主机配置方面的疏漏,达到非法访问网络的目的。

因此,B 关于漏洞类型的描述是错误的。

答案:B。

8-1-6 分析:设计这个例题的目的是加深读者对于欺骗攻击特点的理解。理解欺骗攻

击需要注意以下几个基本问题：

（1）网络攻击者可以通过口令破解、IP欺骗、ARP欺骗、DNS欺骗、Web欺骗、电子邮件欺骗、源路由欺骗、重发攻击与中间人攻击等方法，达到非法访问的目的。这类攻击属于欺骗攻击。

（2）口令攻击是网络攻击最常用的方法。入侵者通过系统常用服务或对网络通信进行监听来搜集账号。当找到主机上的有效账号后，就采用字典穷举法进行攻击，或者通过各种方法获取password文件，然后用口令猜测程序，破译用户账号和密码。

（3）重放攻击可采用不破译密码的方法实施攻击，也叫做IP欺骗攻击。实施IP欺骗的方法是：选定目标主机，发现主机间的信任模式，利用IP、ARP、DNS等手段，冒充被信任主机进入系统，并留下后门供以后使用。

（4）中间人攻击是插入到通信的用户之间，截获加密报文，不做解密的冒充一个用户向另一用户发送，从而骗取信任，解密通信内容的一种攻击形式。

（5）源路由欺骗通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作。

（6）蜜罐是网络安全技术中主动防御攻击与取证的一种技术，不属于网络攻击的内容。

因此，D的描述是错误的。

答案：D。

8-1-7 分析：设计这个例题的目的是加深读者对于DDoS特征的理解。理解DDoS特征，需要注意以下几个基本问题：

（1）拒绝服务攻击（DoS）可以分为两类。一类攻击行为是通过发送一定数量、一定序列的报文，使网络服务器中充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统超出允许的负荷，致使其瘫痪、停止正常的网络服务，并使正在使用的计算机出现无响应、死机的现象。

（2）典型的DDoS攻击采用三层结构：攻击控制层、攻击服务器层、攻击执行器层。DDoS攻击是建立在许多与攻击无关的主机被动地被支配的前提下。在向攻击服务器发出攻击命令的很短时间内，攻击控制台可以立即撤离网络，使得追踪很难实现。

（3）僵尸网络（botnet）攻击是一种典型的DDoS攻击，最严重的攻击事件中，被动受控的主机数量可以高达百万，危害非常严重。有一组数据足以说明僵尸网络的危害。如果一个具有1000个僵尸客户端的小型僵尸网络，每个客户端只用128kbps的发送速率，那么每秒钟就可以产生1.3G的数据量。具备100万个客户端的大型僵尸网络，只要有2～3个僵尸网络发起攻击，足以对一些国家的信息基础设施构成威胁。

因此，B关于botnet规模估计的描述是错误的。

答案：B。

8-1-8 分析：设计这个例题的目的是加深读者对于网络安全服务基本功能的理解。理解网络安全服务的基本功能，需要注意以下几个基本问题：

网络安全服务应该提供以下基本的服务功能：

（1）数据保密。

数据保密服务是防止信息在网络传输过程被非授权用户获取。

（2）认证。

认证服务是用来确定某个通信的参与者的身份是真实的,而且与他所登录的用户身份是一致的,防止出现冒名顶替现象。在网络中两个用户开始通信时,要确认通信双方用户是合法用户。身份认证是检查用户授权、访问控制与审计的前提。

(3) 数据完整。

数据完整服务是用来保证网络中所传输的数据没有被修改、插入或删除,它可以分为有恢复与无恢复服务两类。如果安全系统检测到数据完整性遭到破坏,可以只报告攻击事件已经发生,也可以通过软件或人工干预的方式进行恢复。

(4) 防抵赖。

防抵赖服务是用来保证通信的双方不能对已发送或已接收的信息予以否认。一旦发送方对其发送的数据予以否认,或接收方对已接收的数据进行否认,防抵赖服务可以提供记录,说明否认方是错误的。防抵赖服务对电子商务、电子政务是非常有用的。

(5) 访问控制。

访问控制服务是指控制与限定网络用户对主机系统、网络服务与网络信息资源的访问和使用,防止非授权用户读取、写入、删除或执行文件。

数字签名是一种具体技术,不属于网络安全服务基本功能层面的问题。因此,D 的描述是错误的。

答案:D。

8.2 加密与认证技术

8-2-1 分析:设计这个例题的目的是加深读者对于密钥概念的理解。理解密钥概念需要注意以下几个基本问题:

(1) 密码体制包括基本工作方式以及两个基本要素,即加密/解密算法和密钥。

(2) 加密算法和解密算法的操作通常都是在一组密钥控制下进行。

(3) 对称密码体制的加密密钥和解密密钥是相同的。非对称密码体制的加密密钥和解密密钥是不相同的。

(4) 现代密码学的一个基本原则是:在设计加密系统时,加密算法是可以公开的,真正需要保密的是密钥。一切秘密寓于密钥中。

(5) 从数学的角度来看,改变了密钥,实际上也就改变了明文与密文之间等价的数学函数关系。加密算法是相对稳定的。在这种意义上,可以将加密算法视为常量,而密钥则是一个变量。可以根据事先约好的规则,对应每个新的信息改变一次密钥,或定期更换密钥。

(6) 对于同一种加密算法,密钥的位数越长,破译的困难也就越大,安全性也就越好。密钥位数越多,密钥空间越大,也就是密钥的可能范围也就越大,那么攻击者就越不容易通过蛮力攻击来破译。

从以上讨论中可以看出,B 关于密钥为常量,而加密算法是变量的说法是错误的。

答案:B。

8-2-2 分析:设计这个例题的目的是加深读者对于对称密码体系特点的理解。理解对称密码体系特点,需要注意以下几个基本问题:

(1) 由于通信双方加密与解密时使用同一密钥,因此如果第三方获取该密钥就会造成失密。只要通信双方能确保密钥在交换阶段未泄露,那么就可以保证信息的机密性与完整

性。对称加密技术存在着通信双方之间确保密钥安全交换的问题。

(2) 如果一个用户要与 N 个其他用户进行加密通信时,每个用户对应一把密钥,那么他就需要维护 N 把密钥。当网络中有 N 个用户之间进行加密通信时,则需要有 $N\times(N-1)$ 个密钥,才能保证任意两方之间的通信。

(3) 由于在对称加密体系中加密方和解密方使用相同的密钥,系统的保密性主要取决于密钥的安全性。因此,密钥在加密方和解密方之间的传递和分发必须通过安全通道进行,在公共网络上使用明文传递密钥是不合适的。如果密钥没有以安全方式传送,那么黑客就很可能非常容易地截获密钥。如何产生满足保密要求的密钥,如何安全、可靠地传送密钥是十分复杂的问题。

(4) 密钥管理涉及密钥的产生、分配、存储、销毁。如果设计了一个很好的加密算法,但是密钥管理问题处理不好,则这样的系统同样是不安全的。

因此,B 关于密钥数量的描述是错误的。

答案:B。

8-2-3 分析:设计这个例题的目的是加深读者对于非对称密钥密码体系的理解。理解非对称密钥密码体系特点,需要注意以下几个基本问题:

(1) 在非对称密钥密码体制中,加密的公钥与解密的私钥是不同的。人们可以将加密的公钥公开,谁都可以使用,而解密的私钥只有解密人自己知道。

(2) 由于采用了两个密钥,并且从理论上可以保证从公钥和密文中分析出明文和解密的私钥在计算上是不可行的。以公钥作为加密密钥,接收方使用私钥解密,则可实现多个用户发送的密文,只能由一个持有解密的私钥的用户解读。

(3) 如果以用户的私钥作为加密密钥,而以公钥作为解密密钥,则可以实现由一个用户加密的消息而由多个用户解读,这样非对称密钥密码就可以用于数字签名。

(4) 非对称加密技术可以大大简化密钥的管理,网络中 N 个用户之间进行通信加密,仅仅需要使用 N 对密钥就可以。

因此,C 关于数字签名的描述是错误的。

答案:C。

8-2-4 分析:设计这个例题的目的是加深读者对于 PKI 特点的理解,理解 PKI 的特点,需要注意以下几个基本问题:

(1) PKI 是一种针对电子商务、电子政务应用,利用非对称加密密码体系,提供安全服务的通用性网络安全基础设施。

(2) PKI 系统对用户是透明的,用户在获得加密和数字签名服务时,不需要知道 PKI 是如何管理证书与密钥。

(3) PKI 建立的安全通信信任平台与密钥管理体系,能够为所有的网络应用提供加密与数字签名服务,实现 PKI 系统的关键是密钥的管理。

(4) PKI 主要任务是确定用户可信任的数字身份。这个信任关系是通过公钥证书来实现。公钥证书就是用户身份与所持有公钥的结合,而这种结合关系是由可信任的第三方权威机构——认证中心来确认。

因此,A 关于 PKI 采用的密码体系的描述是错误的。

答案:A。

8-2-5 分析：设计这个例题的目的是加深读者对于PKI工作原理的理解。理解PKI的基本工作原理，需要注意以下几个基本问题：

(1) PKI的认证中心(CA)产生用户之间通信所使用的非对称加密的公钥与私钥对，并存储在证书数据库中。

(2) 当用户A希望与用户B通信时，用户A向CA申请下载包含用户A密钥的数字证书。认证中心的注册认证(RA)中心在确认了用户A合法身份之后，将数字证书发送给用户A。用户A有加密用的密钥。

(3) 用户B可以通过数字证书的方式获得对应的公钥。在用户A向用户B发送用私钥加密和数字签名的文件时，可以用公钥验证文件的合法性。

(4) 在PKI系统中，CA中心与RA中心负责用户身份的确认、密钥的分发与管理、证书撤销。

(5) 实际的PKI系统中不可能只有一个CA中心。多个CA中心之间必然存在一个信任关系模型。信任模型建立的目的是：确保一个认证机构颁发的证书，能够被另一个认证机构的用户的信任。

因此，D关于CA中心的描述是错误的。

答案：D。

8-2-6 分析：设计这个例题的目的是加深读者对于数字签名基本概念的理解。理解数字签名基本概念，需要注意以下几个基本问题：

(1) 亲笔签名是用来保证文件或资料真实性的一种方法。

(2) 数字签名需要实现以下三项主要功能：

① 接收方可以核对发送方对报文的签名，以确定对方的身份。

② 发送方在发送报文之后无法对发送的报文及签名抵赖。

③ 接收方无法伪造发送方的签名。

(3) 目前广泛应用的数字签名算法是消息摘要MD5算法。

(4) MD5算法实际上没有对任何数据进行加密或修改，只是生成一个用于判断数据完整性与真实性的散列值。

因此，D关于MD5算法作用的描述是错误的。

答案：D。

8.3 网络安全协议

8-3-1 分析：设计该例题的目的是加深读者对IPSec的主要特征的理解。在讨论IPSec的主要特征时，需要注意以下几个主要问题：

(1) IPSec的安全服务工作在网络层，可以为任何高层协议，如TCP、UDP、ICMP、BGP提供服务。

(2) IPSec不是单一的一种协议，IPSec安全体系主要包括认证头协议、封装安全载荷协议与Internet密钥交换协议等。

(3) IPSec定义了两种保护IP分组的模式：传输模式与隧道模式。

(4) IPSec对于IPv4是可选的，但对IPv6是基本组成部分。

(5) 安全关联是IPSec的工作基础。安全关联是建立网络层安全连接的双方，通过

IKE 协议协商将采用的加密与认证算法的过程。

从以上分析中可以看出，D 关于 IPSec 与 IPv4、IPv6 关系的描述是错误的。

答案：D。

8-3-2 分析：设计该例题的目的是加深读者对 SSL 协议基本概念的理解。在讨论 SSL 协议的基本概念时，需要注意以下几个主要问题：

SSL 协议具有以下几个特点：

(1) SSL 协议尽管可以用于 HTTP、FTP、TELNET 等，但是目前主要应用于 HTTP 协议，为基于 Web 服务的各种网络应用中客户与服务器之间的用户身份认证与安全数据传输提供服务。

(2) SSL 协议处于端系统的应用层与传输层之间，在 TCP 协议之上建立一个加密的安全通道，为 TCP 协议之间传输的数据提供安全保障。

(3) 当 HTTP 协议使用 SSL 协议时，HTTP 的请求、应答报文格式与处理方法不变。不同之处是：应用进程所产生的报文将通过 SSL 协议加密之后，再通过 TCP 连接传送出去；在接收端 TCP 协议将加密的报文传送给 SSL 协议解密之后，再传送到应用层 HTTP 协议。

(4) 当 Web 系统采用 SSL 协议时，Web 服务器的默认端口号从 80 变换为 443；Web 客户端使用 https 取代常用的 http。

(5) SSL 协议包含两个协议：SSL 握手协议(SSL Handshake Protocol)与 SSL 记录协议(SSL Record Protocol)。SSL 握手协议实现双方加密算法的协商与密钥传递，SSL 记录协议定义 SSL 数据传输格式，实现对数据的加密与解密操作。

(6) 1995 年出现的开放源代码 OpenSSL 软件包目前已经推出了 OpenSSL 0.8.1 版，支持 SSLv3 与 TLSv1 版本。

从以上分析中可以看出，B 关于 SSL 协议工作在传输层的描述是错误的。

答案：B。

8-3-3 分析：设计该例题的目的是加深读者对 SET 协议特点的理解。在讨论 SET 协议特点时，需要注意以下几个主要问题：

(1) SET 协议已经成为目前公认的最成熟的应用层电子支付安全协议。

(2) SET 协议采用数字信封技术保护交易中数据交换的秘密性。

(3) SET 协议通过 CA 中心，实现对通信实体之间、持卡人身份、商家身份、支付网关身份的认证。

(4) SET 协议通过数字签名，确保系统内部交换信息在传输过程中不被篡改与伪造。

(5) SET 协议规定了加密算法的应用、证书授权过程与格式、信息交互过程与格式、认证信息格式等，使不同软件厂商开发的软件具有兼容性和互操作性，并能够运行在不同的硬件和操作系统平台上。

从以上分析中可以看出，C 关于 SET 身份认证关系的描述是错误的。

答案：C。

8.4 防火墙技术

8-4-1 分析：设计这个例题的目的是加深读者对于防火墙功能的理解。理解防火墙功能需要注意以下几个基本问题：

(1) 检查所有从外部网络进入内部网络的数据包。

(2) 检查所有从内部网络流出到外部网络的数据包。

(3) 执行安全策略,限制所有不符合安全策略要求的数据包通过。

(4) 具有防攻击能力,保证自身的安全性。

因此,C关于防火墙功能的描述是错误的。

答案:C。

8-4-2 分析:设计这个例题的目的是加深读者对于防火墙系统结构的理解。理解防火墙系统结构,需要注意以下几个基本问题:

(1) 构成防火墙系统的两个基本部件是包过滤路由器和应用级网关。

(2) 包过滤路由器按照系统设置的分组过滤规则,检查每个分组的源IP地址、目的IP地址,决定该分组是否应该转发。分组过滤规则涉及TCP报头的部分或全部内容。

(3) 包过滤路由器将分析所接收的包,按照每条包过滤的规则加以判断,凡是符合包转发规则的包被转发,凡是不符合包转发规则的包被丢弃。

(4) 包过滤路由器是被保护的内部网络与外部不信任网络之间的第一道防线。

(5) 最简单的防火墙由一个包过滤路由器组成。包过滤路由器通常也称做屏蔽路由器。而复杂的防火墙系统是由包过滤路由器和应用级网关组合而成。由于组合方式有多种,因此防火墙系统的结构也有多种形式。

因此,B关于分组过滤规则与IP地址关系的描述是错误的。

答案:B。

8.5 入侵检测技术

8-5-1 分析:设计这个例题的目的是加深读者对于入侵检测基本概念的理解。理解入侵检测基本概念,需要注意以下几个基本问题:

(1) 入侵检测系统(IDS)是对计算机和网络资源的恶意使用行为进行识别的系统。

(2) 研究入侵检测技术的目的是:监测和发现可能存在的攻击行为,包括来自系统外部的入侵行为和来自内部用户的非授权行为,并采取相应的防护手段。

(3) 入侵检测系统的基本功能包括:

- 监控、分析用户和系统的行为。
- 检查系统的配置和漏洞。
- 评估重要的系统和数据文件的完整性。
- 对异常行为的统计分析,识别攻击类型,并向网络管理人员报警。
- 对操作系统进行审计、跟踪管理,识别违反授权的用户活动。

因此,D关于IDS功能的描述是错误的。

答案:D。

8-5-2 分析:设计这个例题的目的是加深读者对于入侵检测系统结构的理解。理解入侵检测系统结构,需要注意以下几个基本问题:

(1) 事件发生器(event generators)。

CIDF通用框架结构中的事件(event)可以是网络中的数据包,也可以是从系统日志等其他途径得到的信息。事件发生器产生的事件可能是经过协议解析的数据包,或者是从日

志文件中提取的相关部分。

(2) 事件分析器(event analyzers)。

事件分析器根据事件数据库的入侵特征描述、用户历史行为模型等,解析事件发生器产生的事件,得到格式化的描述,判断什么是合法的,什么是非法的。

(3) 响应单元(response units)。

响应单元则是对分析结果做出反应的功能单元,它可以做出切断连接、改变文件属性或报警等响应。

(4) 事件数据库(event databases)。

事件数据库存放攻击类型数据或者检测规则,它可以是复杂的数据库,也可以是简单的文本文件。事件数据库储存有入侵特征描述、用户历史行为等模型和专家经验。

因此,A 关于入侵检测系统结构的描述是错误的。

答案:A。

8-5-3 分析:设计这个例题的目的是加深读者对于入侵检测方法的理解。理解入侵检测方法,需要注意以下几个基本问题:

(1) 通过对各种事件进行分析,从中发现违反安全策略的行为是入侵检测系统的核心功能。入侵检测方法可以分为异常检测、误用检测及两种方法结合。

(2) 异常检测是指已知网络的正常活动状态,如果当前网络状态不符合正常的状态,则认为有攻击发生。异常检测系统的关键是建立一个对应正常网络活动的特征原型。所有与特征原型中差别很大的行为均被视为异常。显然,入侵活动与异常活动是有区别的,关键问题是如何选择一个区分异常事件的阈值,才能减少漏报和误报的问题。在用户数量多、运作状态复杂的环境中,试图用逻辑方法明确划分正常行为和异常行为是非常困难的。

(3) 误用检测系统是建立在使用某种模式或特征描述方法,能够对任何已知攻击进行表达的理论基础上。误用检测系统的主要问题是:如何确定所定义的攻击特征模式可以覆盖与实际攻击相关的所有要素,以及如何对入侵活动的特征进行匹配。根据入侵者在入侵时的某些行为过程的特征,建立一种入侵行为模型。如果用户的行为或者行为过程与入侵方案模型一致,则判定入侵发生。

因此,D 关于异常活动都是入侵活动的描述是错误的。

答案:D。

8-5-4 分析:设计这个例题的目的是加深读者对于 IDS 分类的理解。理解 IDS 分类,需要注意以下几个基本问题:

(1) 按照检测的对象和基本方法,IDS 可以分为基于主机的 IDS、基于网络的 IDS 与分布式 IDS。

(2) 基于主机的 IDS 主要任务是保护所在的计算机系统,它一般是以系统日志、应用程序日志为数据源。由于基于主机的 IDS 审计的信息来自于单个的主机,它能确定是哪个进程和用户参与对操作系统的一次攻击,并且能"预见"此次攻击的后果,因此它能够做到相对准确和可靠。

(3) 基于网络的 IDS 一般是通过将 Ethernet 网卡设置成"混杂模式"来收集在网上出现的数据帧,使用原始的数据帧作为数据源,采用以下基本的识别技术:

- 模式、表达式或字节匹配。

- 频率或阈值。
- 事件的相关性。
- 统计意义上的非正常现象检测。

这类系统一般是被动地在网络上监听整个网段的数据流,通过分析和异常检测或特征比对,发现网络入侵事件。

(4)分布式IDS一般是由分布在网络上不同位置的检测部件组成,分别进行数据采集、数据分析,通过中心控制系统进行数据汇总、分析、产生入侵报警信号。分布式IDS不仅能检测针对单个主机的入侵,也能检测针对整个网络上主机的入侵。

因此,C关于基于网络IDS检测能力的描述是错误的。

答案:C。

8.6 网络业务持续性规划技术

8-6-1 分析:设计这个例题的目的是加深读者对于网络文件备份基本方法的理解。理解网络文件备份基本方法,需要注意以下几个基本问题:

对于网络管理员来说,网络文件备份是日常的网络管理工作任务之一。网络文件备份要解决以下几个基本问题:选择备份设备、选择备份程序与建立备份制度。

(1)选择备份设备应根据网络文件系统的规模、文件的重要性来决定。

(2)选择备份程序应注意备份程序支持哪种网络操作系统;支持哪种备份设备;备份设备是安装在服务器上,还是安装在工作站上;能否从单个文件服务器的备份设备上完成多个服务器的备份。

(3)建立备份制度需要为文件备份制定一张计划表,规定多长时间做一次网络备份以及是否每次都要备份所有文件。建立备份制度计划表的第一件事是选择需要备份的文件和备份的时间。

(4)在考虑备份方法时一定要注意,备份的目的是为了能够恢复系统,因此用户一定要知道以下几点:在系统遭到破坏的情况下,需要多长时间才可能恢复系统;怎样备份才可能在恢复系统时数据损失最少。

因此,D关于备份作用的描述是错误的。

答案:D。

8-6-2 分析:设计这个例题的目的是加深读者对于业务可持续性规划技术的理解。理解业务可持续性规划技术,需要注意以下几个基本问题:

(1)规划的方法学问题。

业务持续性规划技术是一项要求很高的工作,它的作用是保护公司与部门最为重要的财产——信息。规划的方法学是要从目前已经存在的多种实际应用的方案中,总结出基本的方法,包括风险分析、用户需求、设计流程、可选的方案,实施时机、责任人与步骤,以及安全评价方法等。

(2)风险分析方法。

业务持续性规划是针对某个公司或机构的网络信息系统,那么第一步的工作应该是风险分析。针对网络信息系统的风险分析方法,实际上是从广义的角度去评估可能存在的漏洞、漏洞产生的原因,以及在系统恢复中应给予的优先级。风险分析方法应该从定性分析进

入定量分析，而目前风险分析方法仍不成熟，需要深入地进行研究。

（3）数据恢复规划。

对于公司来说，成功的业务持续性评价标准是：如何在最短的时间内恢复对数据的访问能力。业务持续性规划的主要任务就是：如何缩短对数据访问的恢复时间。

数据恢复规划涉及数据分类、鉴别数据的影响等级、网络分级备份策略、存储手段与制度、异地存储的安全性、远程镜像、记录存储的备份方案，以及实施数据恢复、终端用户的恢复策略、应急决策机制、数据恢复评估的规划。

因此，D关于数据恢复规划的描述是不完整的。

答案：D。

8.7 网络防病毒技术

8-7-1 分析：设计这个例题的目的是加深读者对于恶意代码特洛伊木马特点的理解。理解特洛伊木马特点，需要注意以下几个基本问题：

（1）特洛伊木马程序是一种嵌入一些正常软件中的恶意软件，是专为欺骗用户，让用户以为它是友好程序而设计。

（2）木马程序不改变或感染其他文件，它只是伪装成一种正常程序，随着其他的一些应用程序装到用户计算机中，但是用户并不知道程序是什么。

（3）很多木马程序就是后门程序。后门（backdoor）程序使黑客可以访问客户计算机系统，而不会让用户或管理员知道。

因此，D关于特洛伊木马传播特点的描述是错误的。

答案：D。

8-7-2 分析：设计这个例题的目的是加深读者对于垃圾邮件定义的理解。理解垃圾邮件定义，需要注意以下几个基本问题：

垃圾邮件的定义是：

（1）收件人事先没有提出要求或者不同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件。

（2）收件人无法拒收的电子邮件。

（3）隐藏发件人身份、地址、标题等信息的电子邮件。

（4）含有虚假的信息源、发件人、路由等信息的电子邮件。

因此，B关于垃圾邮件特征的描述是错误的。

答案：B。

第三部分　综合练习——术语解析

从给出的26个定义中挑出20个，并将标识定义的字母填在对应术语前的空格位置。

（1）________后门攻击　　（2）________拒绝服务攻击

（3）________篡改信息　　（4）________数据保密服务

（5）________身份认证　　（6）________入侵检测系统

（7）________防抵赖　　（8）________欺骗攻击

(9) ________隧道模式
(10) ________僵尸网络
(11) ________认证中心
(12) ________公钥基础设施
(13) ________数字签名
(14) ________包过滤路由器
(15) ________漏洞攻击
(16) ________木马
(17) ________公钥加密体制
(18) ________防火墙
(19) ________异常检测
(20) ________业务持续性规划

A. 目的节点没有接收到应该接收的信息,信息在传输过程中丢失。
B. 信息遭到修改或插入欺骗性的信息,使得接收的信息是错误的。
C. 对网络攻击者的统称。
D. 利用网络中硬件或软件存在的缺陷,非法访问网络、窃取信息的现象。
E. 通过口令破解等方法达到非法侵入网络系统的目的。
F. 通过消耗网络带宽或系统资源,导致网络瘫痪或停止正常网络服务的攻击。
G. 控制大量分布在不同地理位置的主机,同时向一台目标主机发起攻击的现象。
H. 通过调试后门等方式,绕过网络防护系统的攻击方式。
I. 防止信息在网络传输过程中被非法用户窃取。
J. 检查用户权限,实施访问控制与审计的功能。
K. 保证网络中所传输的数据不被修改、插入或删除的服务。
L. 保证通信的双方不能对已发送或已接收的信息予以否认的服务功能。
M. 控制与限定网络用户对主机系统、网络服务与网络信息资源的访问和使用的功能。
N. 由安全网关执行 IPSec 协议的工作模式。
O. 加密用的公钥与解密用的私钥不同的加密体系。
P. 利用公钥加密和数字签名技术建立的提供安全服务的基础设施。
Q. 产生用户之间通信所使用的非对称加密的公钥与私钥对的部门。
R. 用户申请下载包含用户密钥的数字证书的部门。
S. 网络环境中利用非对称加密算法保证文件发送人身份真实性的方法。
T. 保护内部网络资源不被外部非授权用户使用和非法用户攻击的网络设备。
U. 建立检查进出内部网络数据包合法性,标准网络区域安全的方法。
V. 按照系统内部设置的分组过滤规则决定该分组是否应该转发的网络设备。
W. 对计算机和网络资源的恶意使用行为进行识别的系统。
X. 根据已知网络的正常活动状态来判断攻击行为的方法。
Y. 对突发事件对网络与信息系统影响的预防技术。
Z. 假扮成其他的程序,依靠用户的信任去激活的恶意程序。

参考答案

(1) H　(2) F　(3) B　(4) I　(5) J
(6) W　(7) L　(8) E　(9) N　(10) G
(11) Q　(12) P　(13) S　(14) V　(15) D
(16) Z　(17) O　(18) T　(19) X　(20) Y

参 考 文 献

[1] Andrew S. Tanenbaum. Computer Networks. 5th Edition. Prentice-Hall PTR,2011.
[2] Behrouz A. Forouzan,etc. TCP/IP Protocol Suite. McGraw-Hill Inc. ,2000.
[3] Eric A. Hall. Internet Core Protocols: The Definitive Guide. O'Reilly Inc. ,2000.
[4] 吴功宜. 计算机网络高级教程. 2 版. 北京：清华大学出版社,2015.
[5] 吴功宜. 计算机网络高级软件编程技术. 2 版. 北京：清华大学出版社,2011.
[6] 吴功宜. 网络安全高级软件编程技术. 北京：清华大学出版社,2007.
[7] 吴功宜. 计算机网络与互联网技术研究、应用和产业发展. 北京：清华大学出版社,2008.
[8] 吴功宜. 计算机网络技术教程——自顶向下分析与设计方法. 北京：机械工业出版社,2009.
[9] 吴功宜. 计算机网络课程设计. 2 版. 北京：机械工业出版社,2015.
[10] 吴英. TCP/IP 详解 卷 1：协议. 北京：机械工业出版社,2016.